2014-03-26

The Cyber Security Mess

Garfinkel, Simson L.

Monterey, California. Naval Postgraduate School

The Cyber Security Mess

Simson L. Garfinkel
Associate Professor, Naval Postgraduate School

March 26, 2014

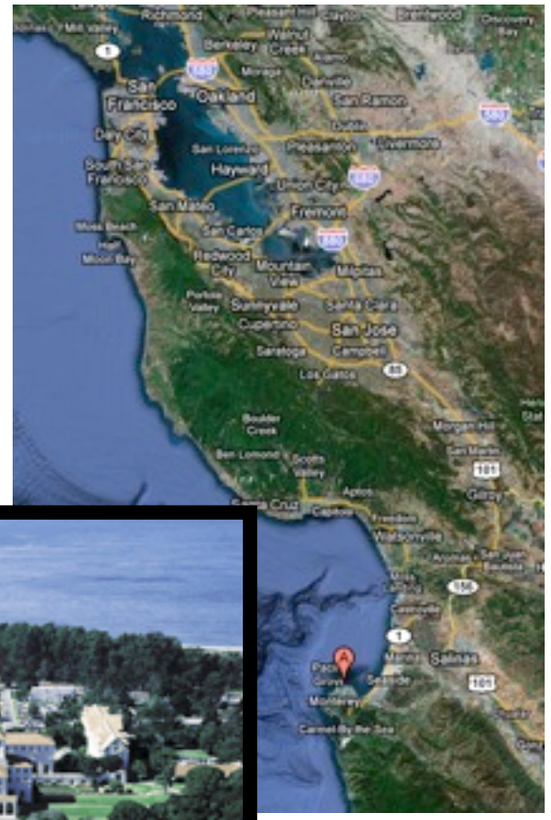
DISCLAIMER:

"The views expressed in this document are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government."

NPS is the Navy's Research University.

Monterey, CA — 1500 students

- US Military & Civilian (Scholarship for Service & SMART)
- Foreign Military (30 countries)



Graduate Schools of
Operational & Information Sciences (GSOIS)

- Computer Science
- Defense Analysis
- Information Sciences
- Operations Research
- Cyber Academic Group

National Capital Region (NCR) Office

- 900 N Glebe (Ballston)/Virginia Tech building

"The Cyber Security Risk", *Communications of the ACM*, June 2012, 55(6)

DOI:10.1145/2184319.2184330

Simson L. Garfinkel

Inside Risks

The Cybersecurity Risk

Increased attention to cybersecurity has not resulted in improved cybersecurity.

THE RISK OF being "hacked"—whatever that expression actually means—is at the heart of our civilization's chronic cybersecurity problem. Despite decades of computer security research, billions spent on secure operations, and growing training requirements, we seem incapable of operating computers securely.

There are weekly reports of penetrations and data thefts at some of the world's most sensitive, important, and heavily guarded computer systems. There is good evidence that global interconnectedness combined with the proliferation of hacker tools means that today's computer systems are actually *less secure* than equivalent systems a decade ago. Numerous breakthroughs in cryptography, secure coding, and formal methods notwithstanding, cybersecurity is getting worse as we watch.

So why the downward spiral? One reason is that cybersecurity's goal of reducing successful hacks creates a large target to defend. Attackers have the luxury of choice. They can focus their efforts on the way our computers represent data, the applications that process the data, the operating systems on which those applications run, the networks by which those applications communicate, or any other area that is possibly subverted. And faced with a system that is beyond one's technical hacking skills, an attacker can go around the security perimeter and use a range of other techniques, including social engineering, supply-chain insertion, or even kidnapping and extortion.

ILLUSTRATION BY YAREK WASZUL

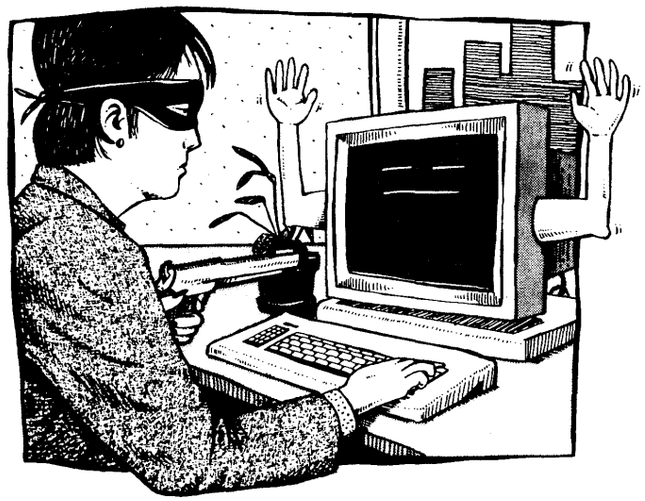
It may be that cybersecurity appears to be getting worse simply because society as a whole is becoming much more dependent upon computers. Even if the vulnerability were not increasing, the successful hacks can have significantly more reach today than a decade ago.

Views of Cybersecurity

The breadth of the domain means many different approaches are being proposed for solving the cybersecurity problem:

- Cybersecurity can be viewed solely as an *insider problem*. What is needed, say advocates, are systems that prevent

I have spent 25 years trying to secure computers...



An Introduction to Computer Security
[Part 1]

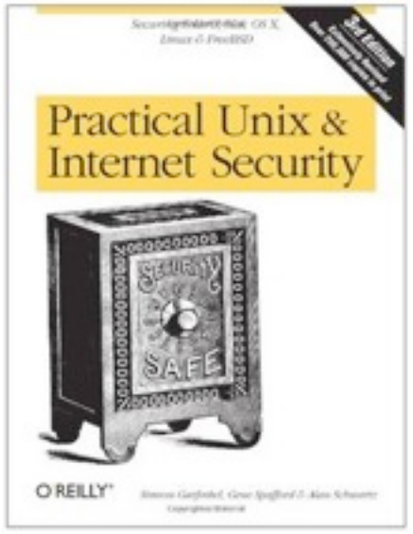
Simson L. Garfinkel

"Spies," "vandals," and "crackers" are out there, waiting to get into—or destroy—your databases.

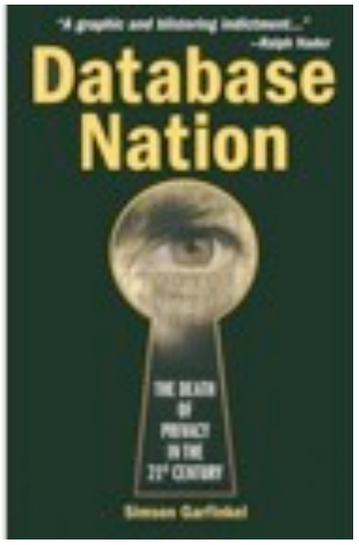
LAWYERS MUST UNDERSTAND issues of computer security, both for the protection of their own interests and the interests of their clients. Lawyers today must automatically recognize insecure computer systems and lax operating procedures in the same way as lawyers now recognize

39

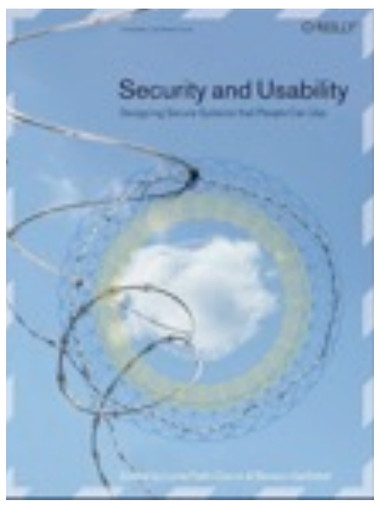
Sept. 1987



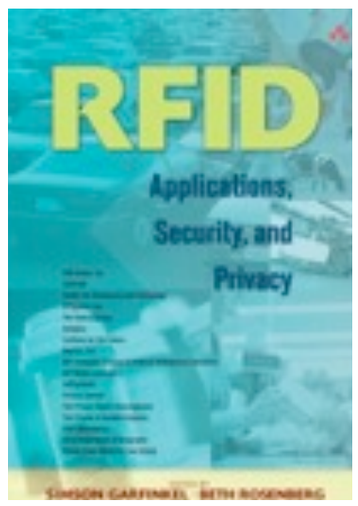
1991



2000



2006

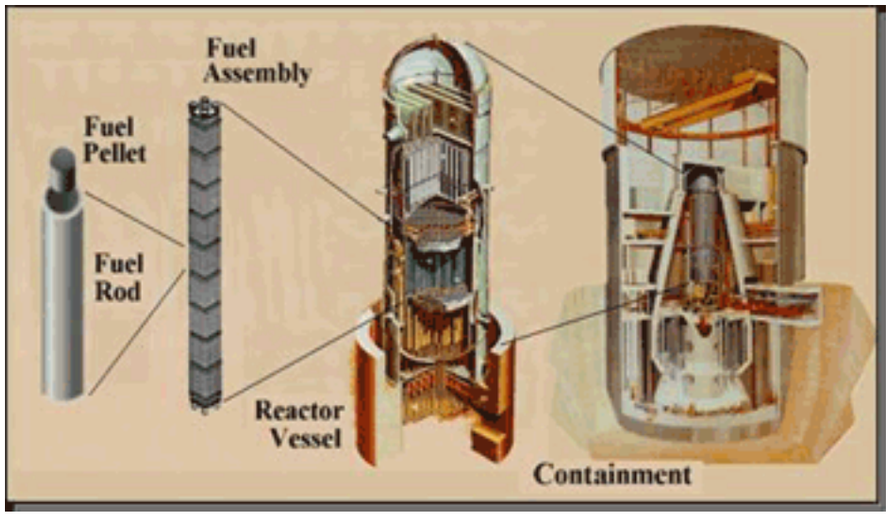


2006

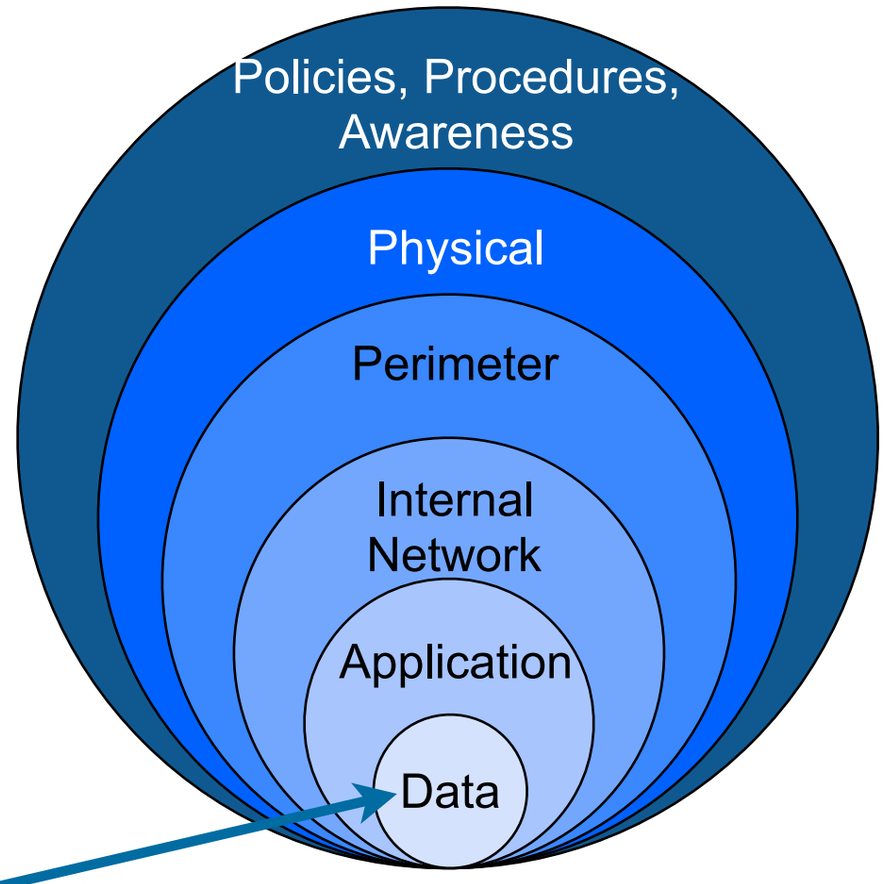
Today's systems are less secure than those of the 1970s.

The lack of security is **inherent** in modern information systems.

- Attack is **easier and cheaper** than defense.
- Cyber "defense in depth" does not work
  — *a single vulnerability compromises.*



Defense in depth of nuclear reactors
http://www.nrc.gov/about-nrc/regulatory/research/soar/soarca-accident-progression.html



Cyber can directly target inner defenses

It's easier to break things than to fix them.

May 2013 —
$45 million stolen from US banks with phony ATM cards

RISK ASSESSMENT / SECURITY & HACKTIVISM

How hackers allegedly stole “unlimited” amounts of cash from banks in just hours

Feds accuse eight men of participating in heists that netted $45 million.

by **Dan Goodin** - May 9 2013, 3:45pm EDT

BLACK HAT HACKING 55

Wikipedia

Federal authorities have accused eight men of participating in 21st-Century Bank heists that netted a whopping $45 million by hacking into payment systems and eliminating withdrawal limits placed on prepaid debit cards.

The eight men formed the New York-based cell of an international crime ring that organized and executed the hacks and then used fraudulent payment cards in dozens of countries to withdraw the loot from automated teller machines, federal prosecutors alleged in court papers unsealed Thursday. In a matter of hours on two separate occasions, the eight defendants and their confederates withdrew about $2.8 million from New York City ATMs alone. At the same times, "cashing crews" in cities in at least 26 countries withdrew more than $40 million in a similar fashion.

April 2013 — AP Twitter feed reports White House bombing

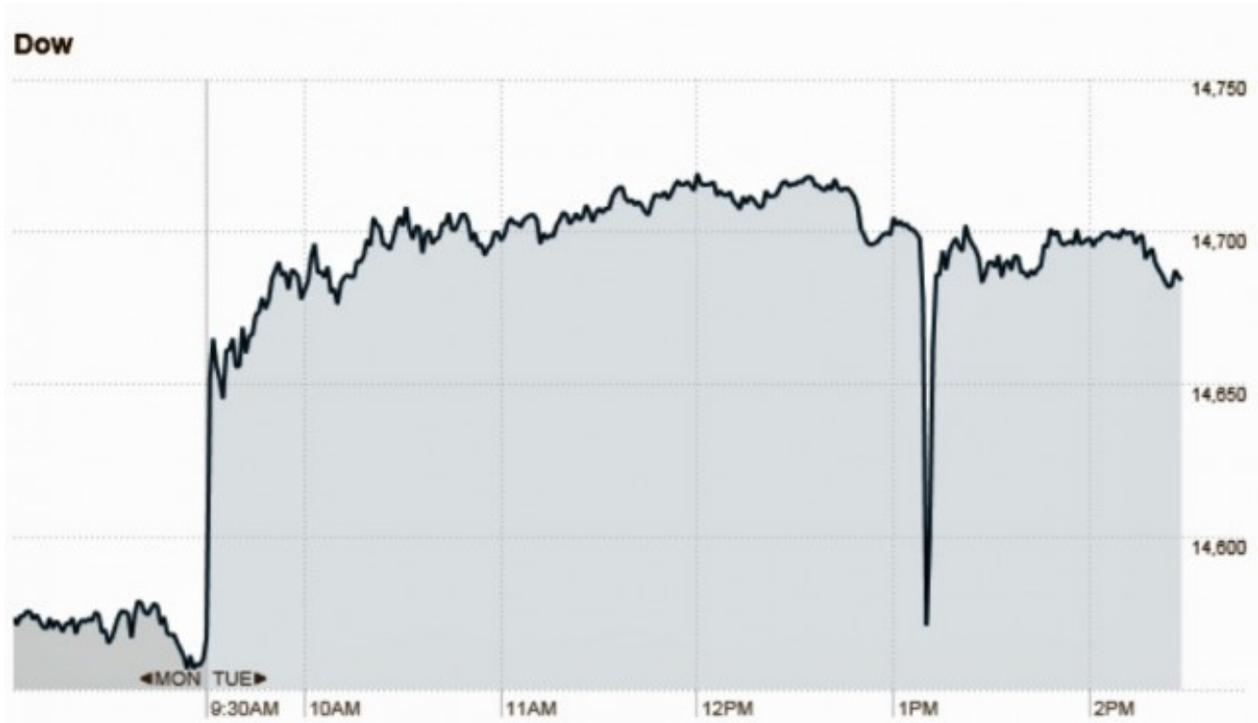
RISK ASSESSMENT / SECURITY & HACKTIVISM

Hacked AP Twitter feed reporting fake White House attack rocks markets

Account compromise comes after AP targeted by malware and phishing e-mails.

by **Dan Goodin** - Apr 23 2013, 3:44pm EDT

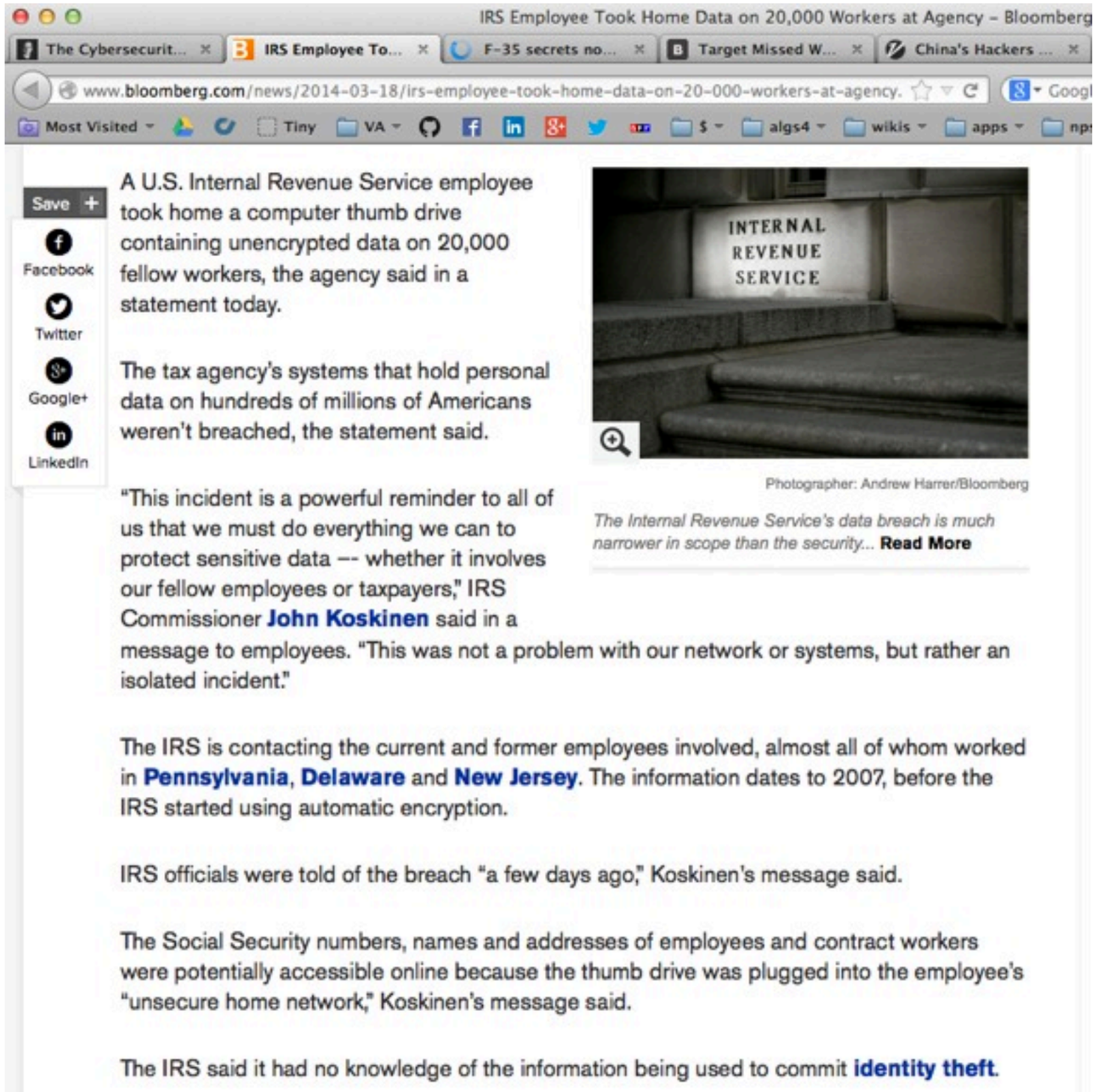
HACKING INTERNET CRIME 74



The seven-minute drop in the Dow Jones Industrial Average touched off by a single tweet falsely claiming the White House had been bombed. It temporarily wiped out about 1 percent of the average, which can translate into millions or billions of dollars in market capitalization.

Stock prices plunged and then quickly recovered after a Twitter account belonging to the Associated Press was hacked and used to send a bogus report falsely claiming that the White House had been bombed and President Obama was injured.

March 2014:
IRS Employee Took Home Data on 20,000 Workers



IRS Employee Took Home Data on 20,000 Workers at Agency - Bloomberg

The Cybersecurit... | IRS Employee To... | F-35 secrets no... | Target Missed W... | China's Hackers ...

www.bloomberg.com/news/2014-03-18/irs-employee-took-home-data-on-20-000-workers-at-agency.

Most Visited | Tiny | VA | $ | algs4 | wikis | apps

Save +

Facebook

Twitter

Google+

LinkedIn

A U.S. Internal Revenue Service employee took home a computer thumb drive containing unencrypted data on 20,000 fellow workers, the agency said in a statement today.

The tax agency's systems that hold personal data on hundreds of millions of Americans weren't breached, the statement said.

"This incident is a powerful reminder to all of us that we must do everything we can to protect sensitive data -- whether it involves our fellow employees or taxpayers," IRS Commissioner **John Koskinen** said in a message to employees. "This was not a problem with our network or systems, but rather an isolated incident."

Photographer: Andrew Harrer/Bloomberg

The Internal Revenue Service's data breach is much narrower in scope than the security... **Read More**

The IRS is contacting the current and former employees involved, almost all of whom worked in **Pennsylvania**, **Delaware** and **New Jersey**. The information dates to 2007, before the IRS started using automatic encryption.

IRS officials were told of the breach "a few days ago," Koskinen's message said.

The Social Security numbers, names and addresses of employees and contract workers were potentially accessible online because the thumb drive was plugged into the employee's "unsecure home network," Koskinen's message said.

The IRS said it had no knowledge of the information being used to commit **identity theft**.

http://www.bloomberg.com/news/2014-03-18/irs-employee-took-home-data-on-20-000-workers-at-agency.html

March 2014: Stolen F-35 secrets showing up in China's stealth Fighter

F-35 secrets now showing up in China's stealth fighter - Washi

The Cybersecurity Me... | F-35 secrets now sho... | Target Missed Warnin... | China's Hackers to Ta...

www.washingtontimes.com/news/2014/mar/13/f-35-secrets-now-showing-chinas-stealth-fighter/

Most Visited | Tiny | VA | $ | algs4 | wikis

Top Gun takeover: Stolen F-35 secrets showing up in China's stealth fighter

Design data on F-35 stolen in 2007

337 SIZE: + / - PRINT

U.S. Air Force Tech. Sgt. Brian West watches an Air Force F-35 Lightning II joist strike fighter aircraft approach for the first time July 14, 2011, at Eglin Air Force Base, Fla. (U.S. Air Force photo by Samuel King Jr.)

By Bill Gertz - Washington Free Beacon — Thursday, March 13, 2014

A cyber espionage operation by China seven years ago produced sensitive technology and aircraft secrets that were incorporated into the latest version of China's new J-20 stealth fighter jet, according to U.S. officials and private defense analysts.

STORY TOPICS

Technology_Internet

March 2014: Target ignored alarms before hack.

Target Missed Warnings in Epic Hack of Credit Card Data – B

The Cybersecurity Mess – Si... | Target Missed Warnings in E... | China's Hackers to Target U... | For

www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-da

Most Visited | Tiny | VA | $ | algs4 | wikis

Bloomberg.com | Businessweek.com | Bloomberg TV | Premium

BloombergBusinessweek
Technology

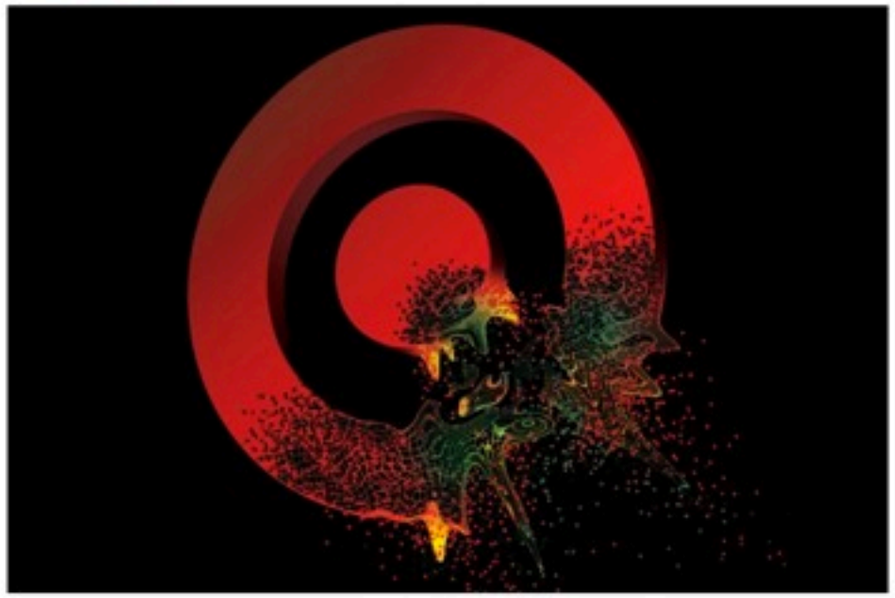
Global Economics | Companies & Industries | Politics & Policy | Technology | Markets & Finance | Innovation & Design | Lifestyle

Features

Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It

By Michael Riley, Ben Elgin, Dune Lawrence, and Carol Matlack | March 13, 2014

SEND TO kindle



(Corrects to identify Romania in a map accompanying the story.)

The biggest retail hack in U.S. history wasn't particularly inventive, nor did it appear destined for success. In the days prior to Thanksgiving 2013, someone installed malware in Target's (TGT) security and payments system designed to steal every credit card used at the company's 1,797 U.S. stores. At the critical moment—when

The cyber security mess: it's technical *and* social.

Most attention is focused on technical issues:

- Malware and anti-viruses
- Access controls, authentication & cryptography
- Supply chain issues
- Cyberspace as a globally connected "domain"

Non-technical issues are at the heart of the cyber security mess.

- Education & career paths
- Immigration
- Manufacturing policy

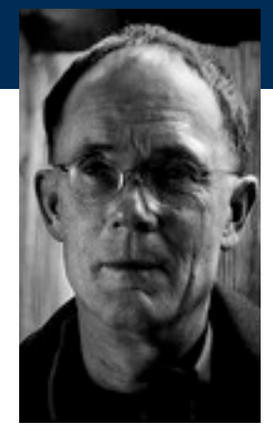
We will do better when we *want* to do better.

What do we know about cyber security today?

Cyber Security... is undefined.

“Cybernetics” **“Cyberspace”**

Norbert Weiner



William Gibson

There is no good definition for “cyber”

- ~~Something having to do with cybernetics~~
- Computers?
- Computer networks?
- Hacking?
- Using “network security” to secure desktops & servers?

There is no way to *measure* the security of a “cyber” system

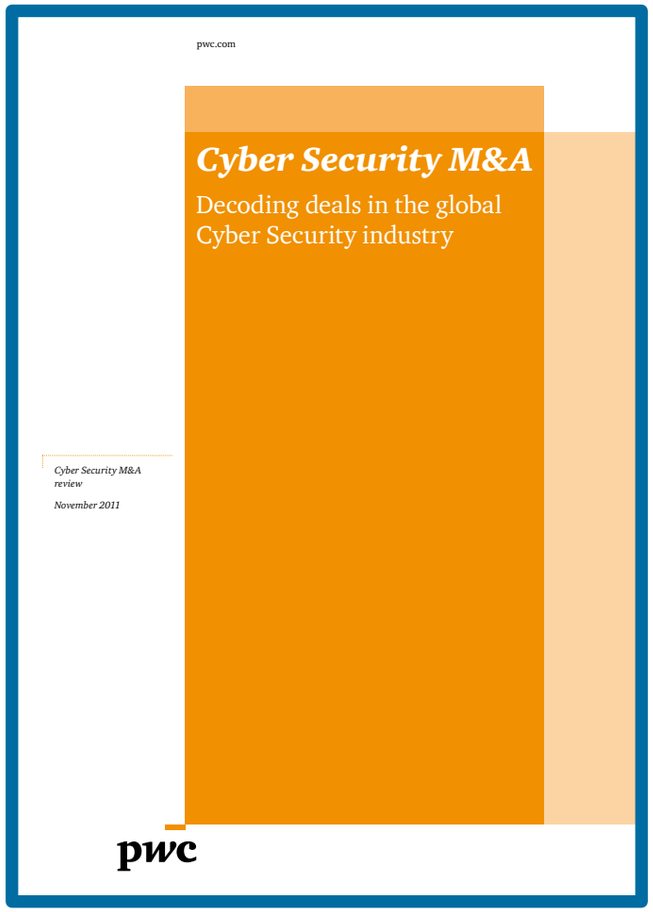
- Which OS is more secure?
- Which computer is more secure?
- Is “open source” more secure?

—A system that seems “more secure”
can suffer a total compromise from a single unknown attack.

We *can* measure expenditures.
Cyber Security is expensive.

Global cyber security spending: $60 billion in 2011

- *Cyber Security M&A,* pwc, 2011


pwc.com

Cyber Security M&A

Decoding deals in the global Cyber Security industry

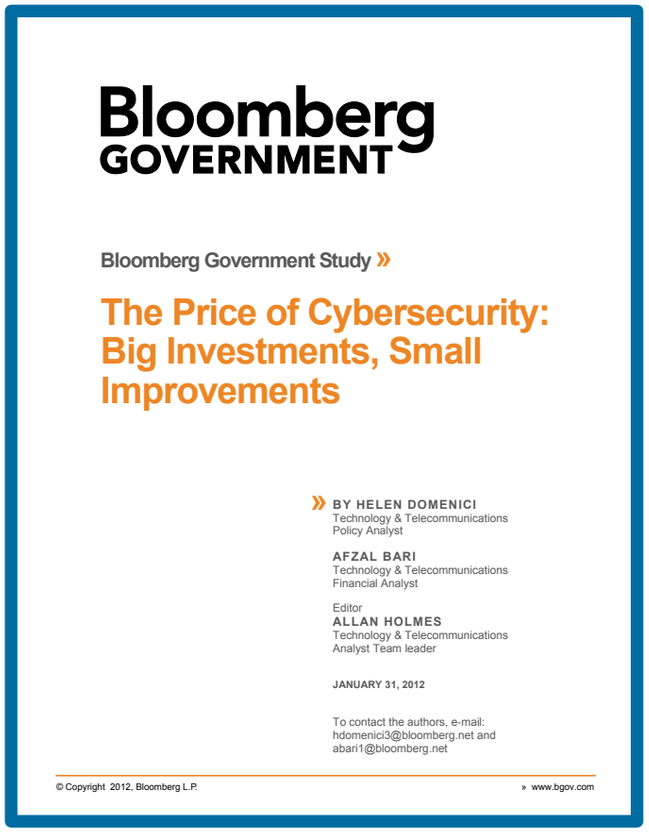
Cyber Security M&A review

November 2011

pwc

172 Fortune 500 companies surveyed:

- Spending $5.3 billion per year on cyber security.
- Stopping 69% of attacks.


Bloomberg GOVERNMENT

Bloomberg Government Study »

The Price of Cybersecurity: Big Investments, Small Improvements

» BY HELEN DOMENICI
Technology & Telecommunications
Policy Analyst

AFZAL BARI
Technology & Telecommunications
Financial Analyst

Editor
ALLAN HOLMES
Technology & Telecommunications
Analyst Team leader

JANUARY 31, 2012

To contact the authors, e-mail:
hdomenici3@bloomberg.net and
abari1@bloomberg.net

© Copyright 2012, Bloomberg L.P. » www.bgov.com

If they raise spending...

- $10.2 billion stops 84%
- $46.67 billion stops 95%
- “highest attainable level”

95% is not good enough.

Spending more money does not make a computer more secure.

Paradox:
Cyber security research makes computers less secure!

—*Data*

—*Encoding*

—*Apps*

—*OS (programs & patches)*

—*Network & VPNs*

—*DNS, DNSSEC*

—*IPv4 / IPv6*

—*Embedded Systems*

—*Human operators*

—*Hiring process*

—*Supply chain*

—*Family members*

The more we learn about securing computers,
the better we get at attacking them

Cyber Security is an “insider problem.”

bad actors

good people with bad instructions

remote access

malware

http://www.flickr.com/photos/shaneglobal/5115134303/

If we can stop insiders, we might be able to secure cyberspace….

—*... but we can’t stop insiders.*

Ames

Hanssen

Manning

Snowden

Cyber Security is a “network security” problem.

We can’t secure the hosts, so secure the network!

- Isolated networks for critical functions.
- Stand-alone hosts for most important functions.

http://www.flickr.com/photos/dungkal/2315647839/

But strong crypto limits visibility into network traffic, and...

... stuxnet shows that there are no isolated hosts.

Iranian President Mahmoud Ahmadinejad inspects nuclear centrifuges

“to a first approximation, every computer in the world is connected to every other computer.”

http://www.nytimes.com/2011/06/30/technology/30morris.html

—Robert Morris (1932-2001), to the National Research Council’s Computer Science and Technology Board, Sept. 19, 1988

“Computer Insecurity”, Peter G. Neumann *Issues In Science & Technology,* Fall 1994

“Action is needed on many fronts to protect computer systems and communications from unauthorized use and manipulation.”

ISSUES ONLINE IN SCIENCE AND TECHNOLOGY

HOME BACK ISSUES

Summer 2003

INTRODUCTION

Daniel Yankelovich — SCIENCE AND THE PUBLIC PROCESS: Why the Gap Must Close (Fall 1984)

RESEARCH & TECHNOLOGY

D. Allan Bromley — Science, Scientists, and the Science Budget (Fall 1992) HTML or PDF

Lewis M. Branscomb — Toward a U.S. Technology Policy (Summer 1991)

Ralph E. Gomory, Harold T.shapiro — A Dialogue on Competitiveness (Summer 1988) HTML or PDF

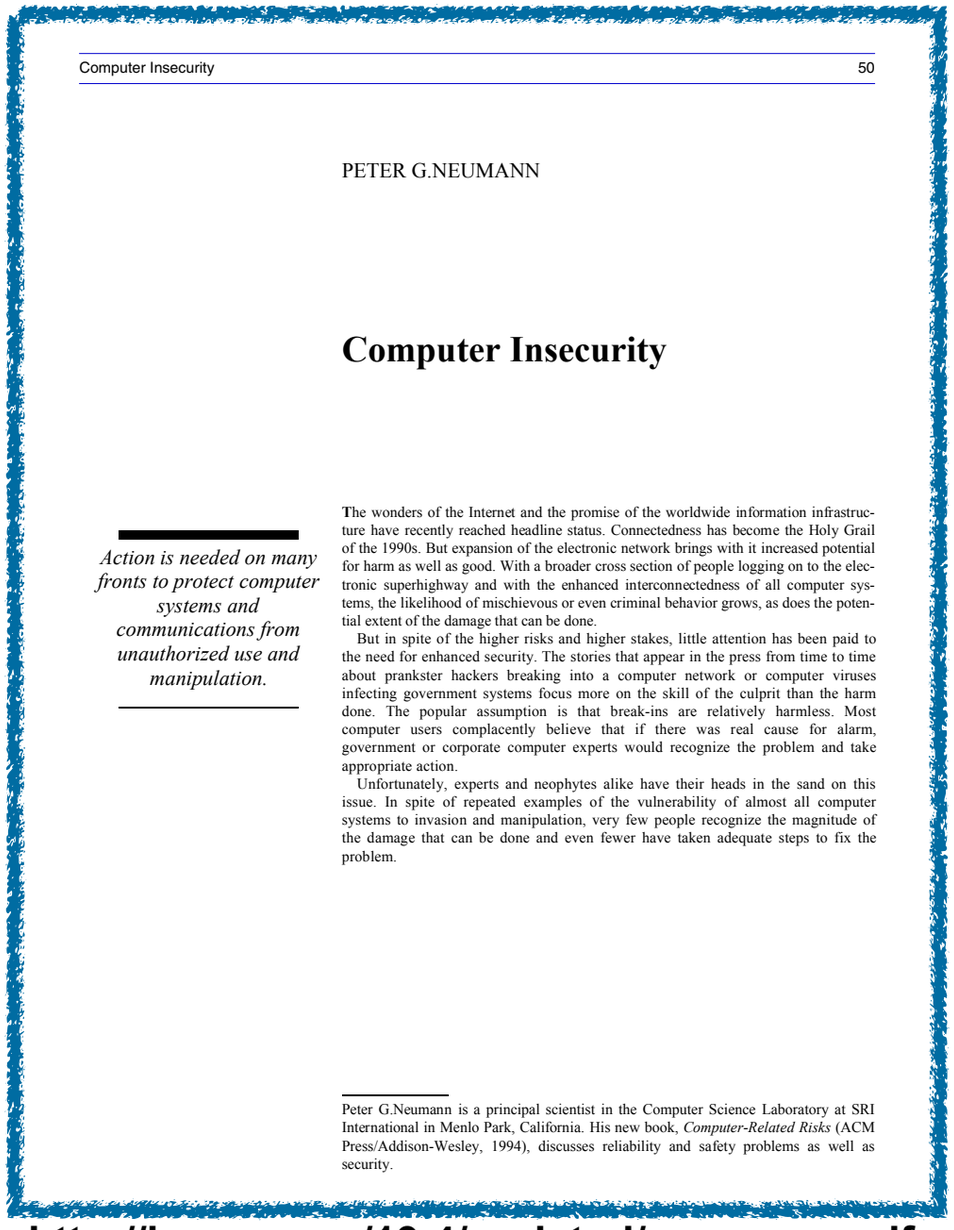
Erich Bloch — MANAGING FOR CHALLENGING TIMES: A National Research Strategy (Winter 1986) HTML or PDF

John A. Armstrong — University Research: New Goals, New Practices HTML or PDF

Roland W. Schmitt — Fulfilling the Promise of Academic Research (Summer 1991) HTML or PDF

Larry R. Johnson — Putting Maglev on Track (Spring 1990) HTML or PDF

http://issues.org/19.4/updated/neumann.html



PETER G.NEUMANN

Computer Insecurity

Action is needed on many fronts to protect computer systems and communications from unauthorized use and manipulation.

The wonders of the Internet and the promise of the worldwide information infrastructure have recently reached headline status. Connectedness has become the Holy Grail of the 1990s. But expansion of the electronic network brings with it increased potential for harm as well as good. With a broader cross section of people logging on to the electronic superhighway and with the enhanced interconnectedness of all computer systems, the likelihood of mischievous or even criminal behavior grows, as does the potential extent of the damage that can be done.

But in spite of the higher risks and higher stakes, little attention has been paid to the need for enhanced security. The stories that appear in the press from time to time about prankster hackers breaking into a computer network or computer viruses infecting government systems focus more on the skill of the culprit than the harm done. The popular assumption is that break-ins are relatively harmless. Most computer users complacently believe that if there was real cause for alarm, government or corporate computer experts would recognize the problem and take appropriate action.

Unfortunately, experts and neophytes alike have their heads in the sand on this issue. In spite of repeated examples of the vulnerability of almost all computer systems to invasion and manipulation, very few people recognize the magnitude of the damage that can be done and even fewer have taken adequate steps to fix the problem.

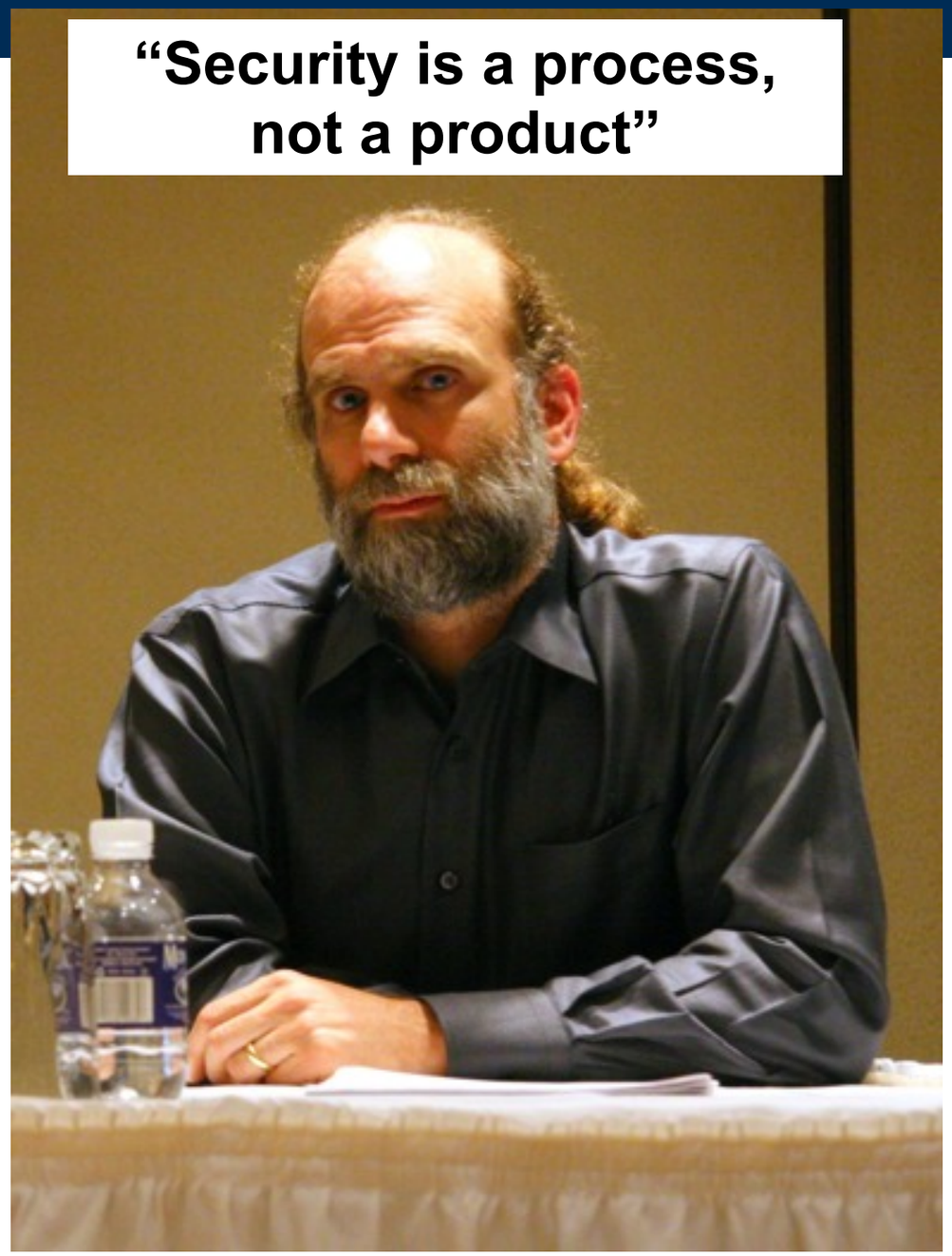
Peter G.Neumann is a principal scientist in the Computer Science Laboratory at SRI International in Menlo Park, California. His new book, *Computer-Related Risks* (ACM Press/Addison-Wesley, 1994), discusses reliability and safety problems as well as security.

http://issues.org/19.4/updated/neumann.pdf

Cyber Security is a “process” problem.

Security encompasses all aspects of an organization’s IT and HR operations.

Microsoft Security Development Lifecycle



http://en.wikipedia.org/wiki/File:Bruce_Schneier_1.jpg

—*Few organizations can afford SDL.*

—~~*Windows 7*~~ *Windows 8 is still hackable...*

January 2013: Windows RT jailbroken

Microsoft controlled the hardware and the software.

Windows RT — still hacked


nakedsecurity.sophos.com/2013/01/08/windows-rt-jailbroken-shows-its-w

VA wikis apps nps $ TTD Shop Stats news

nakedsecurity

Award-winning news, opinion, advice and research from SOPHOS

malware mac facebook android vulnerability data loss privacy more...

142 Like 4 +1 120 Tweet 14 Share

Smart octogenarian foils scammer w… The TURKTRUST SSL certificate fia…

Windows RT "jailbroken", shows its Windows 8 roots

Join thousands of others, and sign up for Naked Security's newsletter

you@example.com Do it!

Don't show me this again

by Chester Wisniewski on January 8, 2013 | 2 Comments

FILED UNDER: Featured, Microsoft, Vulnerability, Windows

Hey Windows RT, your roots are showing!

Not that it is all that surprising to most people, but the first person to post about jailbreaking a Microsoft Windows RT device says it is a direct port of Windows 8.

Microsoft has gone to some lengths to disguise this fact: no desktop mode applications (except Office, Explorer and IE10), only runs software from the Windows Store and can't

Cyber Security is a money problem.

Security is a cost.....Not an “enabler”

- No ROI

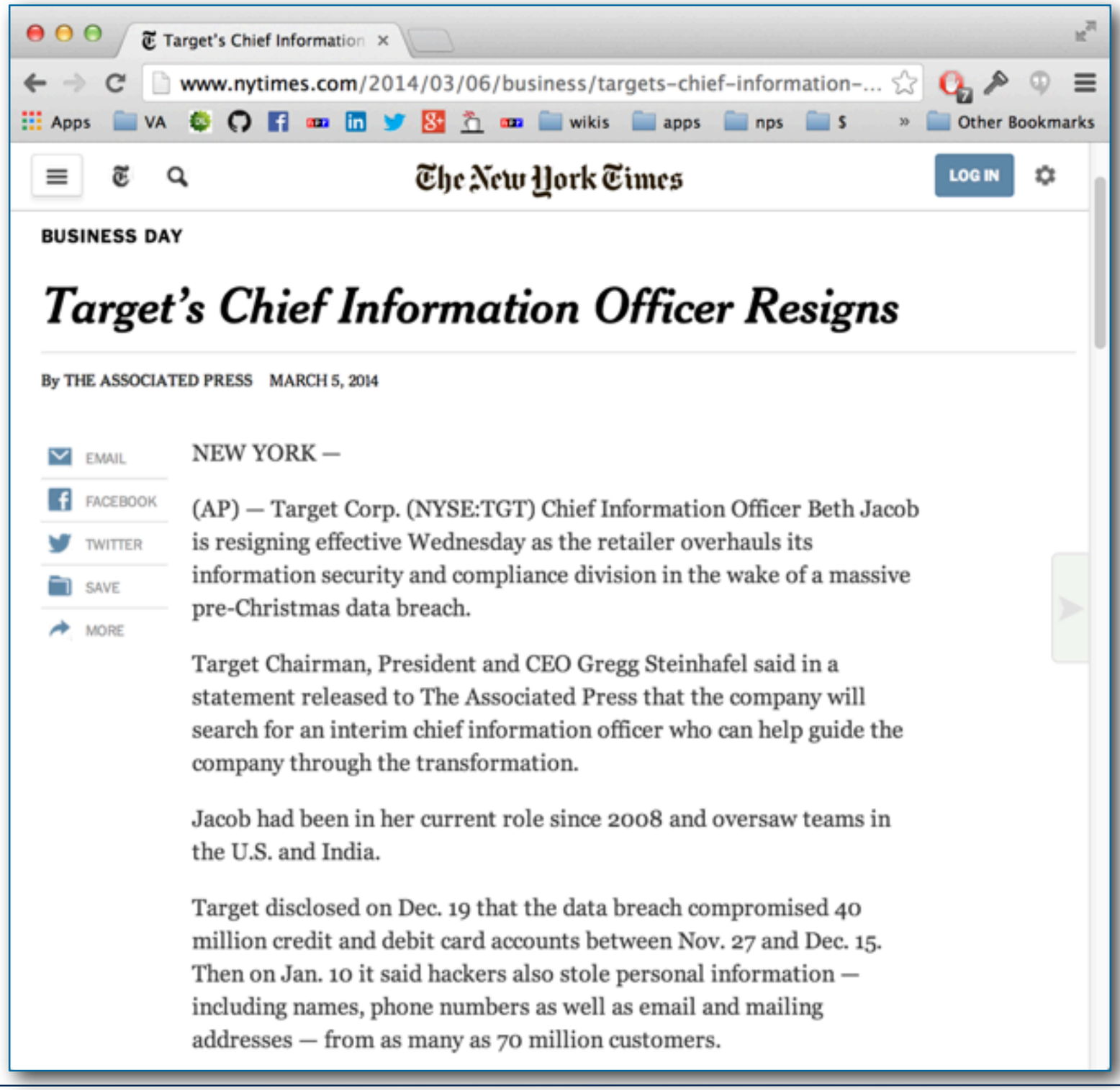
Chief Security Officers are in a no-win situation:

- Security = passwords = frustration
- No reward for spending money to secure the infrastructure
- Money spent on security is “wasted” if there is no attack

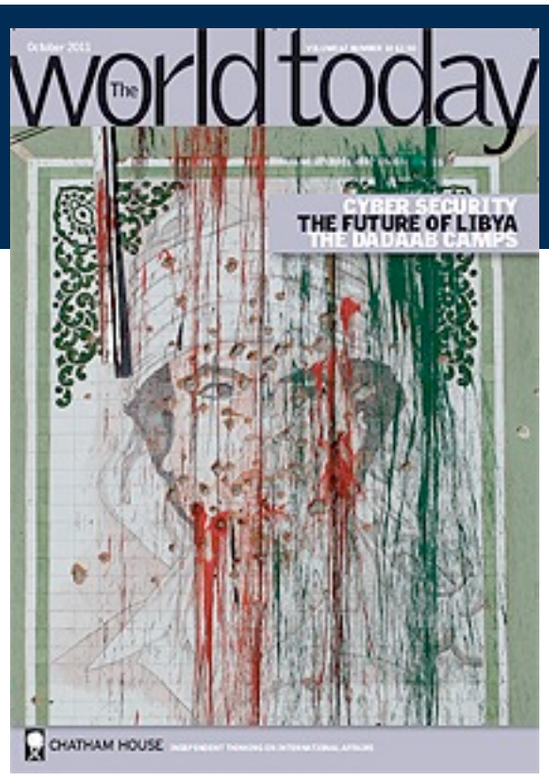
—*“If you have responsibility for security but have no authority to set rules or punish violators, your own role in the organization is to take the blame when something big goes wrong.”*

- Spaf’s first principle of security administration
  Practical Unix Security, 1991

March 5, 2014:
Target's Chief Information Officer resigned



Cyber Security is a “wicked problem”



No clear definition of the wicked problem

—*You don’t understand the problem until you have a solution.*

No “stopping rule”

—*The problem can never be solved.*

Solutions not right or wrong

—*Benefits to one player hurt another — Information security vs. Free speech*

Solutions are “one-shot” — no learning by trial and error

—*No two systems are the same. The game keeps changing.*

Every wicked problem is a symptom of another problem

- Rittel and Webber, “Dilemmas in a General Theory of Planning,” 1973
- Dave Clement, “Cyber Security as a Wicked Problem,” Chatham House, October 2011
  - http://www.chathamhouse.org/publications/twt/archive/view/178579

Why is cyber security *so* hard?

Cyber Security has an active, malicious adversary.

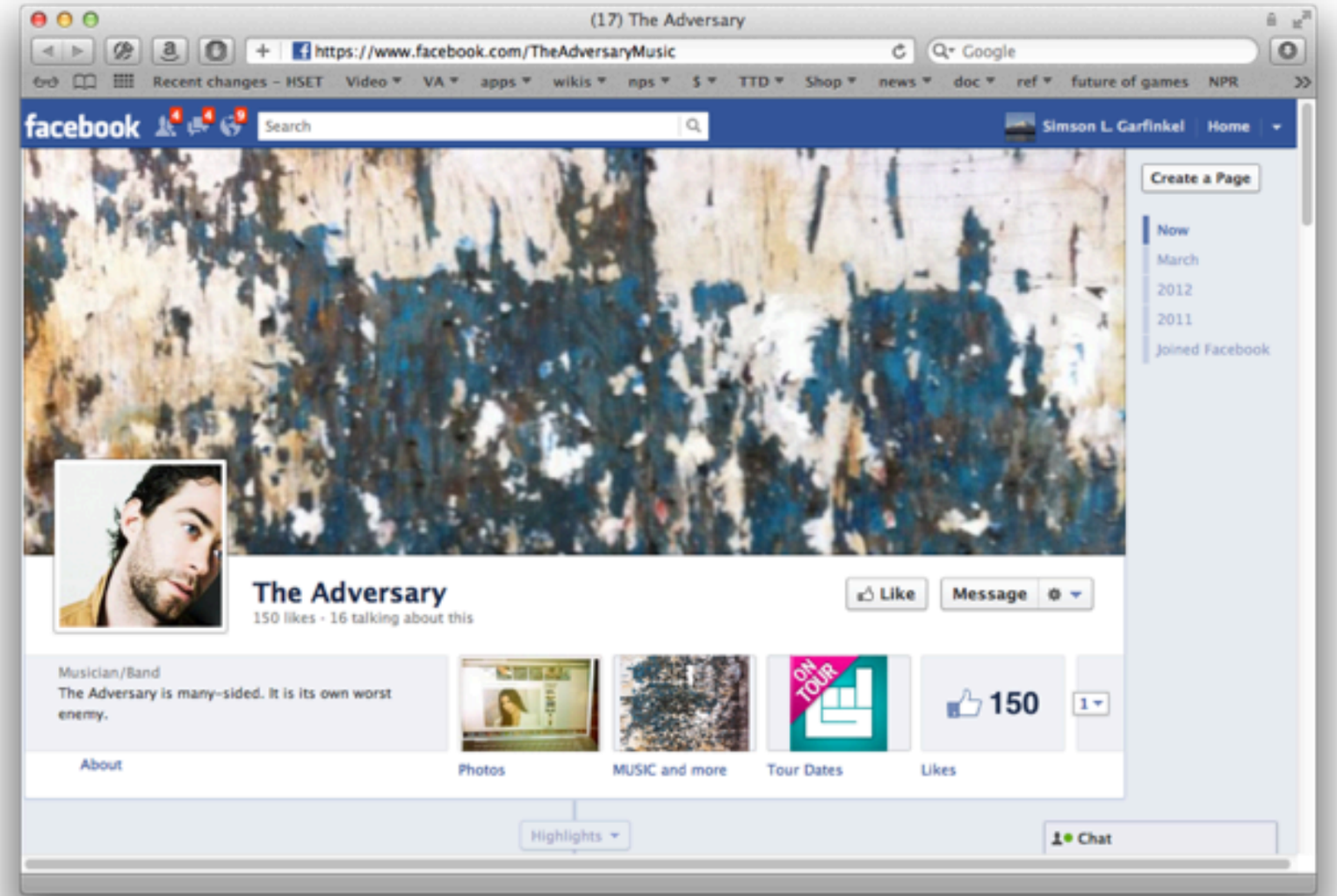
The adversary...

—*Turns your bugs into exploits*

—*Adapts to your defenses*

—*Waits until you make a mistake*

—*Attacks your employees when your systems are secure*



For example...
Compiler bugs are security vulnerabilities!

Compilers are core technology used in software development.

We have seen:

- Optimizations to make programs run faster can become security vulnerabilities
- The same errors are repeatedly made by different programmers

What's difference between a bug and an attack?

—*The programmer's intent.*

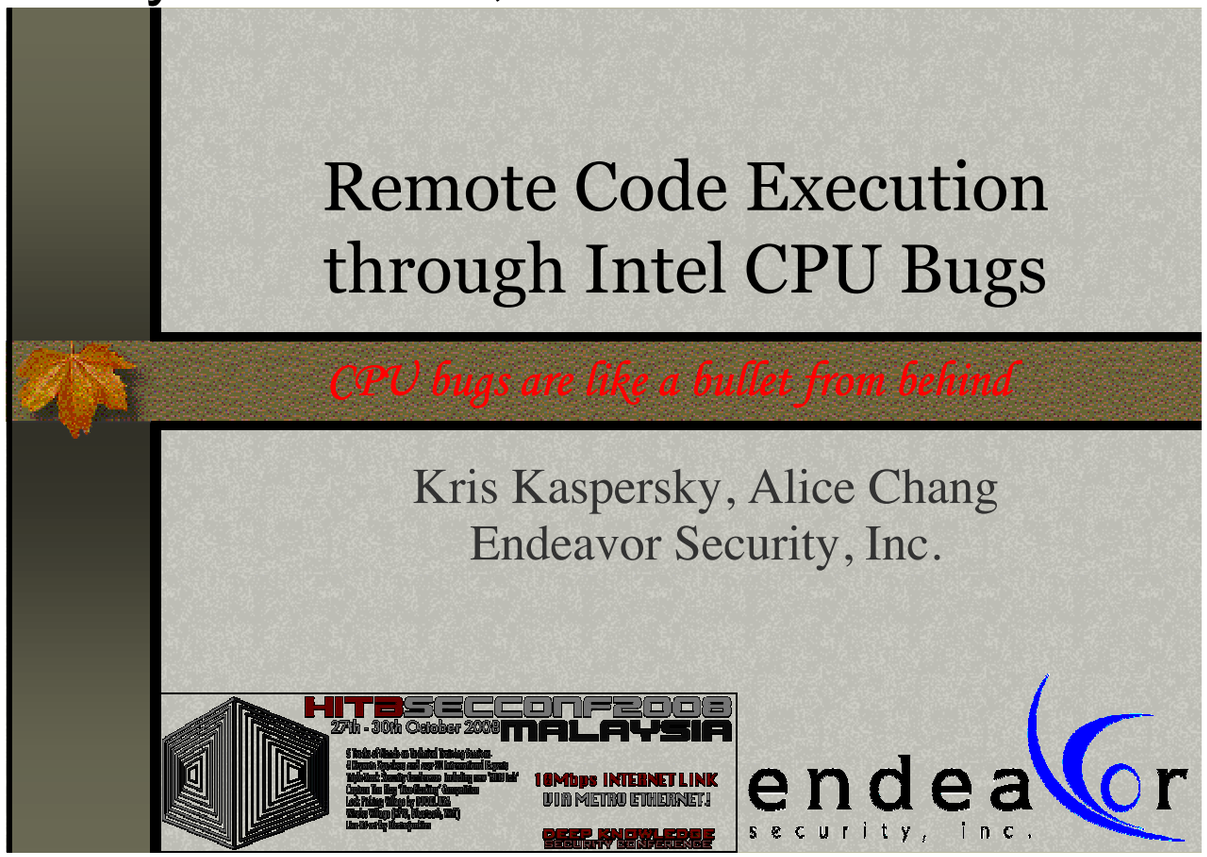
Bugs in CPU silicon are remotely exploitable!

This means:

- Programs that are “secure” on one CPU may be vulnerable on another.
- Auditing the code & the compiler isn’t enough.

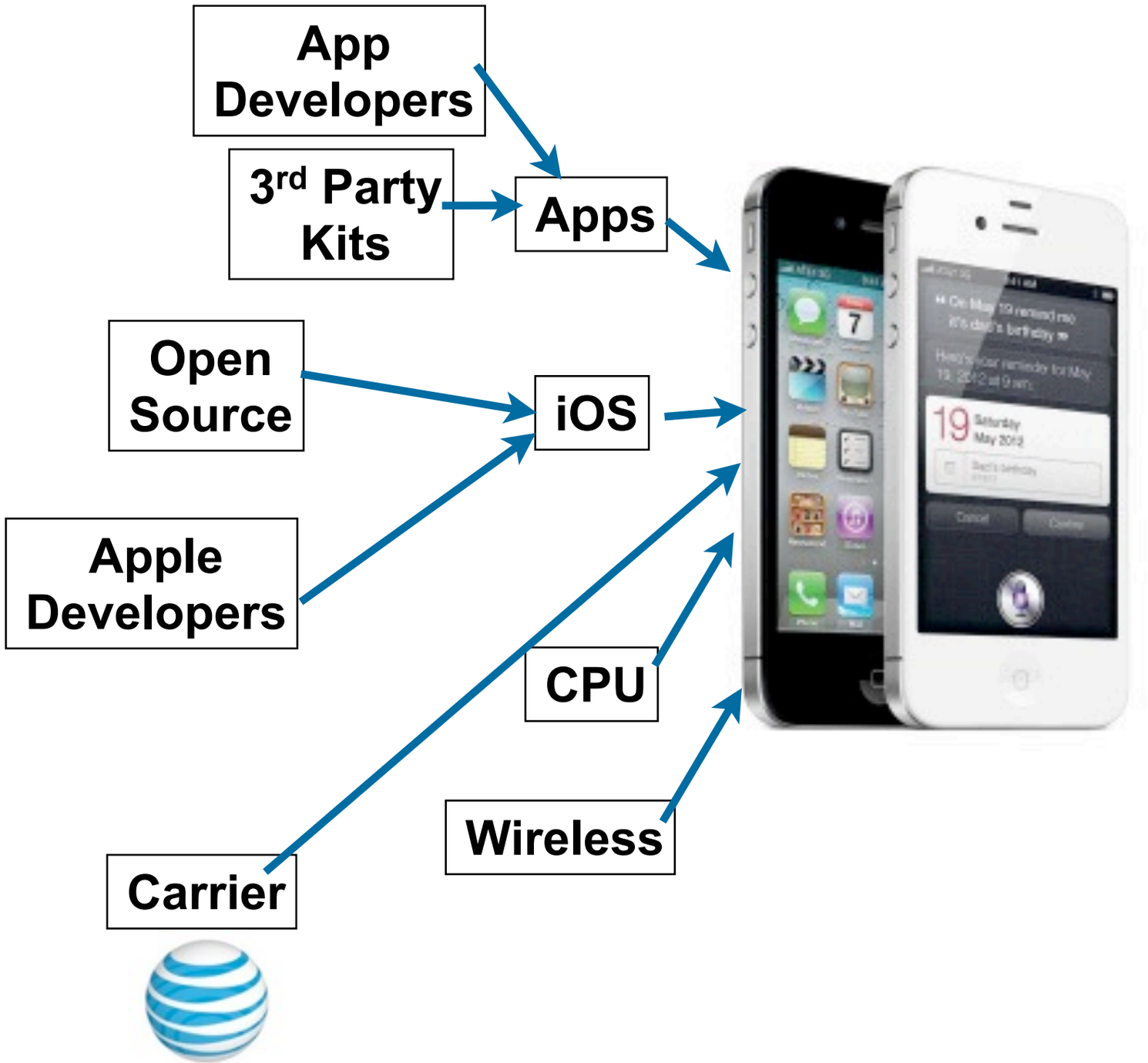
Kaspersky:

- “Fact: malware that uses CPU bugs really does exist;”
- “not apocalypse, just a new threat;”



www.cs.dartmouth.edu/~sergey/cs258/2010/D2T1 - Kris Kaspersky - Remote Code Execution Through Intel CPU Bugs.pdf

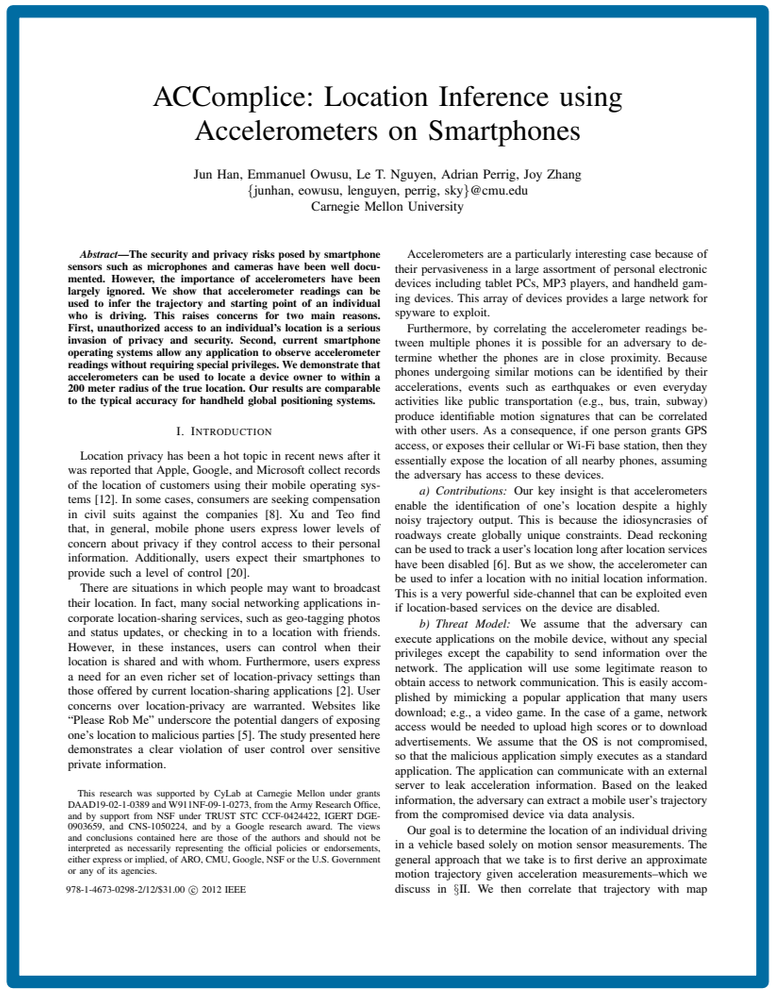
The supply chain creates numerous security vulnerabilities



The attacker is smarter than you are…
… and has more time to find a good attack.

Smartphone designers were sure that there was no privacy leakage in accelerometers. We now know they can:

- Reveal your position
- Reveal your PIN



ACComplice: Location Inference using Accelerometers on Smartphones

Jun Han, Emmanuel Owusu, Le T. Nguyen, Adrian Perrig, Joy Zhang
{junhan, eowusu, lenguyen, perrig, sky}@cmu.edu
Carnegie Mellon University

***Abstract*—The security and privacy risks posed by smartphone sensors such as microphones and cameras have been well documented. However, the importance of accelerometers have been largely ignored. We show that accelerometer readings can be used to infer the trajectory and starting point of an individual who is driving. This raises concerns for two main reasons. First, unauthorized access to an individual's location is a serious invasion of privacy and security. Second, current smartphone operating systems allow any application to observe accelerometer readings without requiring special privileges. We demonstrate that accelerometers can be used to locate a device owner to within a 200 meter radius of the true location. Our results are comparable to the typical accuracy for handheld global positioning systems.**

I. Introduction

Location privacy has been a hot topic in recent news after it was reported that Apple, Google, and Microsoft collect records of the location of customers using their mobile operating systems [12]. In some cases, consumers are seeking compensation in civil suits against the companies [8]. Xu and Teo find that, in general, mobile phone users express lower levels of concern about privacy if they control access to their personal information. Additionally, users expect their smartphones to provide such a level of control [20].

There are situations in which people may want to broadcast their location. In fact, many social networking applications incorporate location-sharing services, such as geo-tagging photos and status updates, or checking in to a location with friends. However, in these instances, users can control when their location is shared and with whom. Furthermore, users express a need for an even richer set of location-privacy settings than those offered by current location-sharing applications [2]. User concerns over location-privacy are warranted. Websites like "Please Rob Me" underscore the potential dangers of exposing one's location to malicious parties [5]. The study presented here demonstrates a clear violation of user control over sensitive private information.

This research was supported by CyLab at Carnegie Mellon under grants DAAD19-02-1-0389 and W911NF-09-1-0273, from the Army Research Office, and by support from NSF under TRUST STC CCF-0424422, IGERT DGE-0903659, and CNS-1050224, and by a Google research award. The views and conclusions contained here are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either express or implied, of ARO, CMU, Google, NSF or the U.S. Government or any of its agencies.

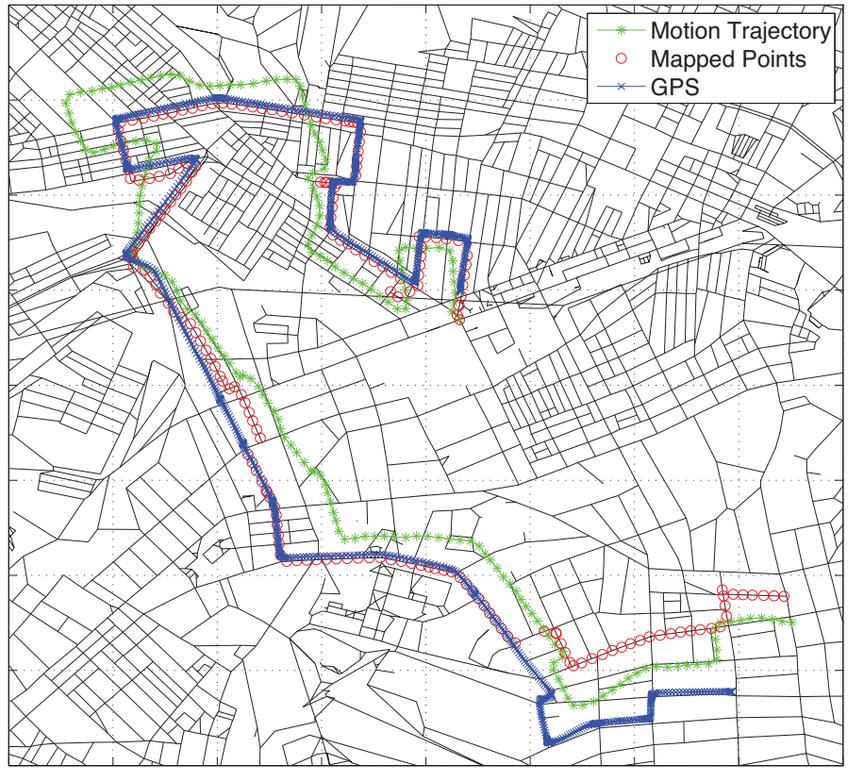
Accelerometers are a particularly interesting case because of their pervasiveness in a large assortment of personal electronic devices including tablet PCs, MP3 players, and handheld gaming devices. This array of devices provides a large network for spyware to exploit.

Furthermore, by correlating the accelerometer readings between multiple phones it is possible for an adversary to determine whether the phones are in close proximity. Because phones undergoing similar motions can be identified by their accelerations, events such as earthquakes or even everyday activities like public transportation (e.g., bus, train, subway) produce identifiable motion signatures that can be correlated with other users. As a consequence, if one person grants GPS access, or exposes their cellular or Wi-Fi base station, then they essentially expose the location of all nearby phones, assuming the adversary has access to these devices.

a) Contributions: Our key insight is that accelerometers enable the identification of one's location despite a highly noisy trajectory output. This is because the idiosyncrasies of roadways create globally unique constraints. Dead reckoning can be used to track a user's location long after location services have been disabled [6]. But as we show, the accelerometer can be used to infer a location with no initial location information. This is a very powerful side-channel that can be exploited even if location-based services on the device are disabled.

b) Threat Model: We assume that the adversary can execute applications on the mobile device, without any special privileges except the capability to send information over the network. The application will use some legitimate reason to obtain access to network communication. This is easily accomplished by mimicking a popular application that many users download; e.g., a video game. In the case of a game, network access would be needed to upload high scores or to download advertisements. We assume that the OS is not compromised, so that the malicious application simply executes as a standard application. The application can communicate with an external server to leak acceleration information. Based on the leaked information, the adversary can extract a mobile user's trajectory from the compromised device via data analysis.

Our goal is to determine the location of an individual driving in a vehicle based solely on motion sensor measurements. The general approach that we take is to first derive an approximate motion trajectory given acceleration measurements–which we discuss in §II. We then correlate that trajectory with map



6 accelerometers no privacy

https://sparrow.ece.cmu.edu/group/pub/han_ACComplice_comsnets12.pdf
Jun Han, Emmanuel Owusu, Thanh-Le Nguyen, Adrian Perrig, and Joy Zhang "ACComplice: Location Inference using Accelerometers on Smartphones" In Proceedings of the 4th International Conference on Communication Systems and Networks (COMSNETS 2012), Bangalore, India, January 3-7, 2012.

Many people liken cyber security to the flu.

DHS calls for “cyber hygiene”

- install anti-virus
- update your OS
- back up key files

—“STOP, THINK, CONNECT”

Another model might be *obesity*....

Making people fat is good business:

- Farm subsidies
- Restaurants
- Healthcare and medical utilization
- Weight loss plans

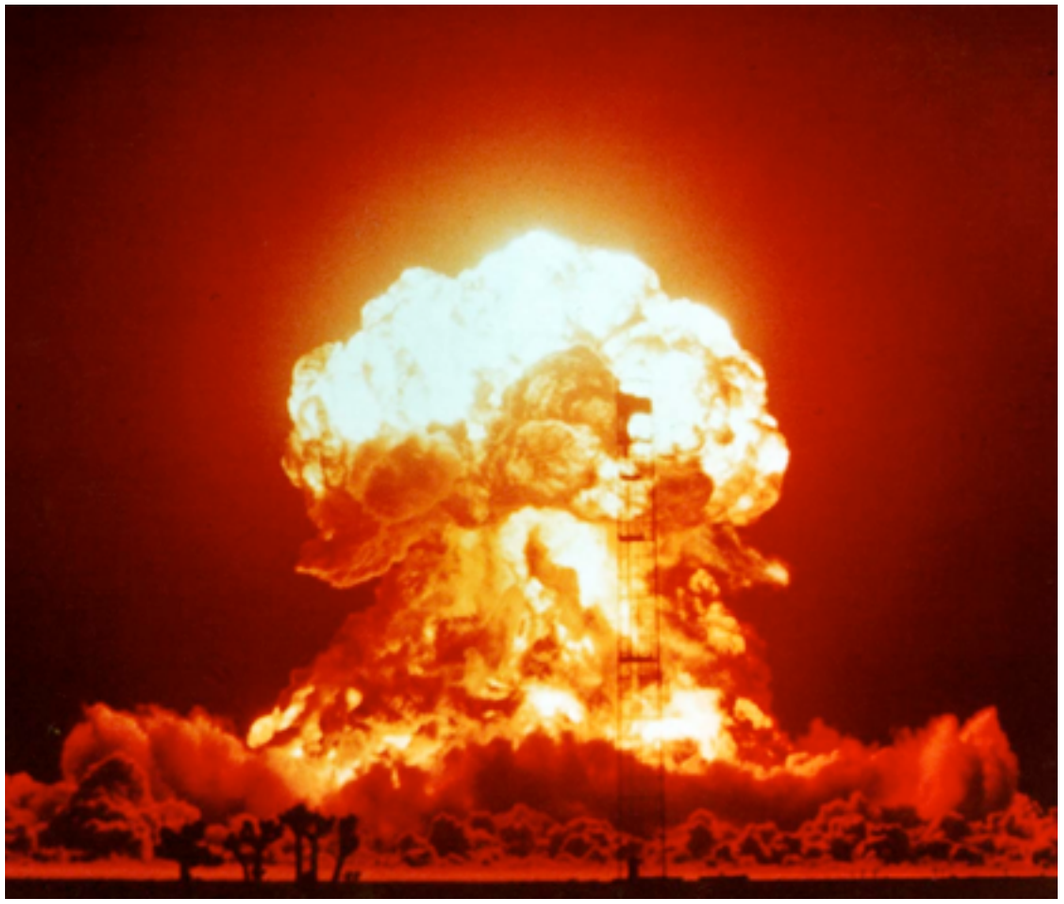
  —*Few make money when Americans stay trim and healthy.*

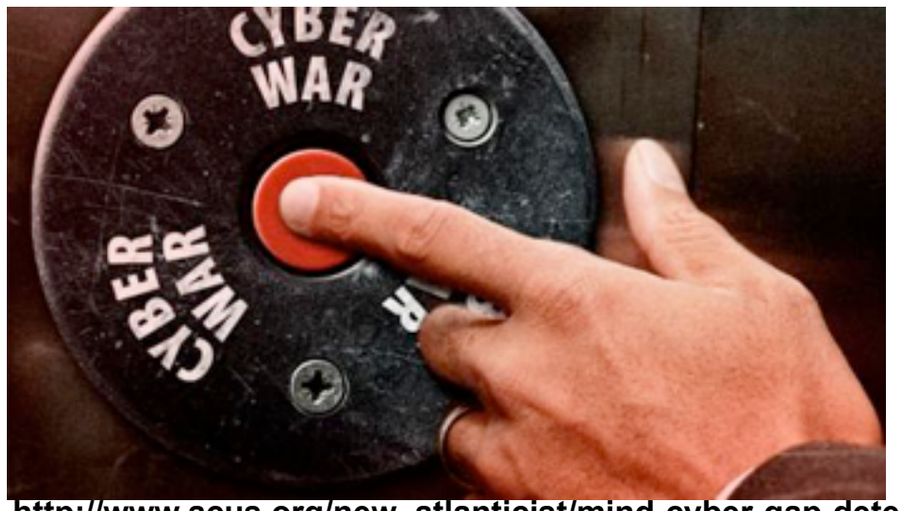
Lax security is also good business:

- Cheaper cost of deploying software
- Private information for marketing
- Selling anti-virus & security products
- Cleaning up incidents

  —*Few benefit from secure computers*

Some people say that cyber war is like nuclear war.





http://www.acus.org/new_atlanticist/mind-cyber-gap-deterrence-cyberspace

http://www.beyondnuclear.org/security/

Biowar may be a better model for cyberwar.

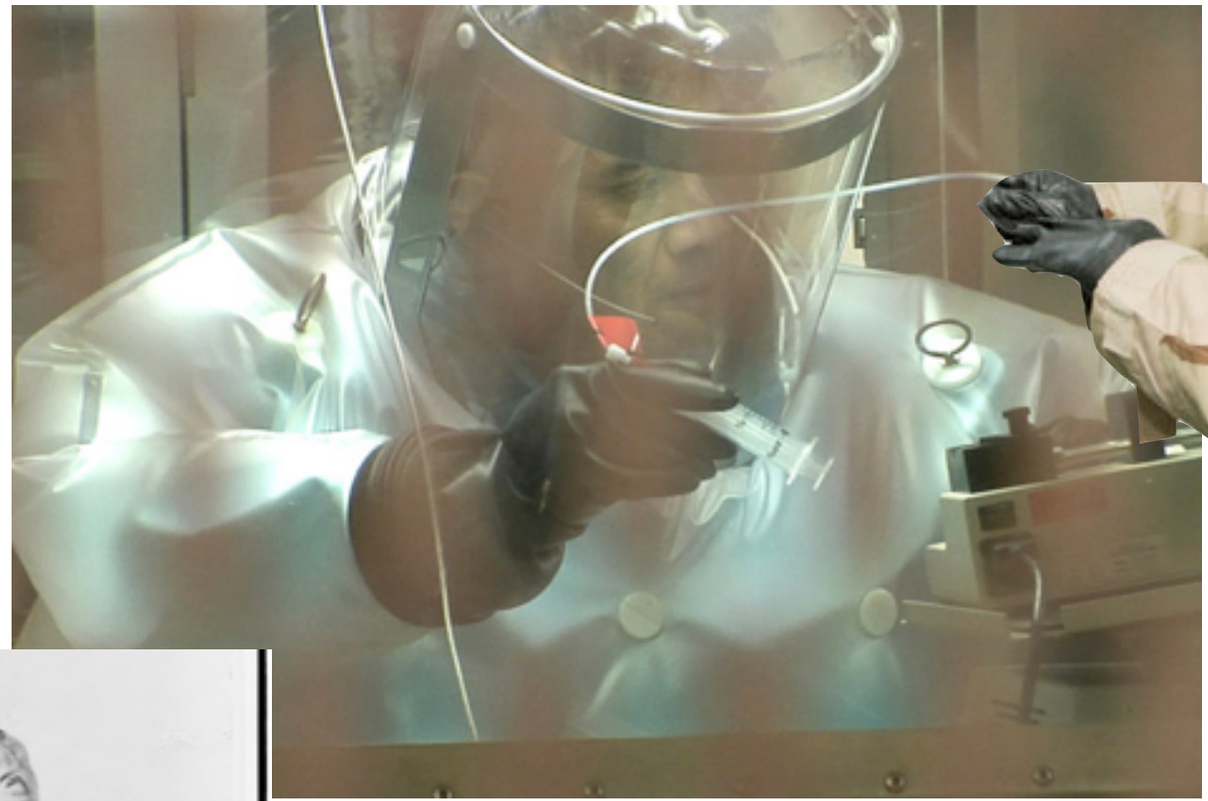
—*Cheap to produce*

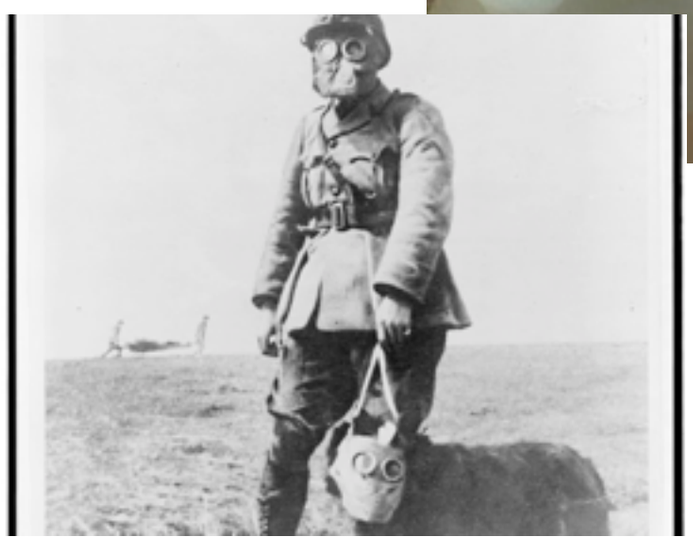
—*Easy to attack*

—*Hard to control*

—*Hard to defend*

—*No clear end*





Security problems are bad for society as a whole...

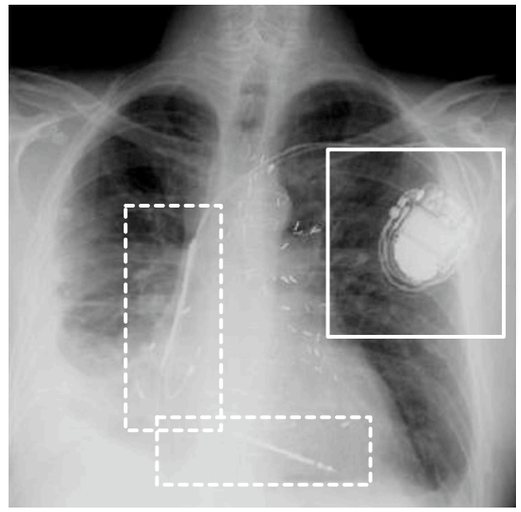
… because [wireless] computers are everywhere.

50 microprocessors per average car

http://www.autosec.org/

- *Comprehensive Experimental Analysis of Automotive Attack Surfaces (2011)*
- *Experimental Security Analysis of a Modern Automobile (2010)*

Remote take-over of EVERY safety-critical system from ANY wired or wireless interface



2008: demonstrated wireless attack on implantable pacemakers

2012: demonstrated wireless attack on insulin pump

DDoS the endocrine system!

[ISN] TV-based botnets? DoS attacks on your fridge? More plausible than you think

From: **InfoSec News <alerts@infosecnews.org>**
Subject: [ISN] TV-based botnets? DoS attacks on your fridge? More plausible than you think
Date: April 23, 2012 3:16:23 AM EDT
To: isn@infosecnews.org

http://arstechnica.com/business/news/2012/04/tv-based-botnets-ddos-attacks-on-your-fridge-more-plausible-than-you-think.ars

By Dan Goodin
ars technica
April 22, 2012

It's still premature to say you need firewall or antivirus protection for your television set, but a duo of recently diagnosed firmware vulnerabilities in widely used TV models made by two leading manufacturers suggests the notion isn't as far-fetched as many may think.

... While poking around a Samsung D6000 model belonging to his brother, he inadvertently discovered a way to remotely send the TV into an endless restart mode that persists even after unplugging the device and turning it back on.

"It wasn't even planned," Auriemma told Ars, referring to the most damaging of his two attacks, which rendered the device useless for three days...

[ISN] ATM Attacks Exploit Lax Security

From: **InfoSec News <alerts@infosecnews.org>**
Subject: [ISN] ATM Attacks Exploit Lax Security
Date: April 23, 2012 3:15:54 AM EDT
To: isn@infosecnews.org
http://www.bankinfosecurity.com/atm-attacks-exploit-lax-security-a-4689

http://krebsonsecurity.com/2011/12/pro-grade-3d-printer-made-atm-skimmer/

By Tracy Kitten
Bank Info Security
April 19, 2012

Lax security makes non-banking sites prime targets for skimming attacks...

Cell phones cannot be secured.

Cell phones have:

- Wireless networks, microphone, camera, & batteries
- Downloaded apps
- Bad crypto

Cell phones can be used for:

- Tracking individuals
- Wiretapping rooms
- Personal data

http://connectedvehicle.challenge.gov/submissions/2706-no-driving-while-texting-dwt-by-tomahawk-systems-llc

How do we address the cybersecurity challenge?

1. Deploy technology that works.

2. Address the non-technical issues.

We have made major advances in cyber security.

Major security breakthroughs since 1980:

- Public key cryptography (RSA with certificates to distribute public keys)
- Fast symmetric cryptography (AES)
- Fast public key cryptography (elliptic curves)
- Easy-to-use cryptography (SSL/TLS)
- Sandboxing (Java, C# and virtualization)
- Firewalls
- BAN logic
- Fuzzing.

None of these breakthroughs has been a “silver bullet,” but they have all helped.

—*“Why Cryptosystems Fail,” Ross Anderson,*
1st Conference on Computer and Communications Security, 1993.
http://www.cl.cam.ac.uk/~rja14/Papers/wcf.pdf

We must continue to deploy technology that works, because adversaries are not all powerful.

Adversaries are impacted by:

- —*Economic factors*
- —*Attention span*
- —*Other opportunities*

You don’t have to run faster than the bear….

http://forums.corvetteforum.com/off-topic/2824193-i-only-have-to-outrun-you-polar-bear-tag.html

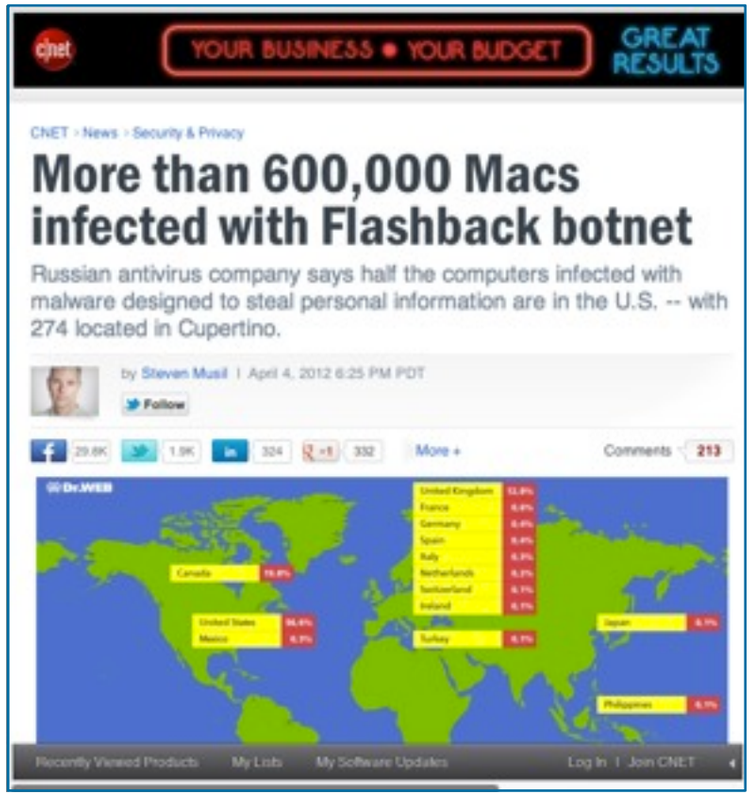
There are solutions to many cyber security problems... We should use them!

30% of the computers on the Internet run Windows XP

- Windows 7 & 8 have vulnerabilities, but they're better.

Apple users don't use anti-virus.

- Yes, Apple tries to fix bugs, but

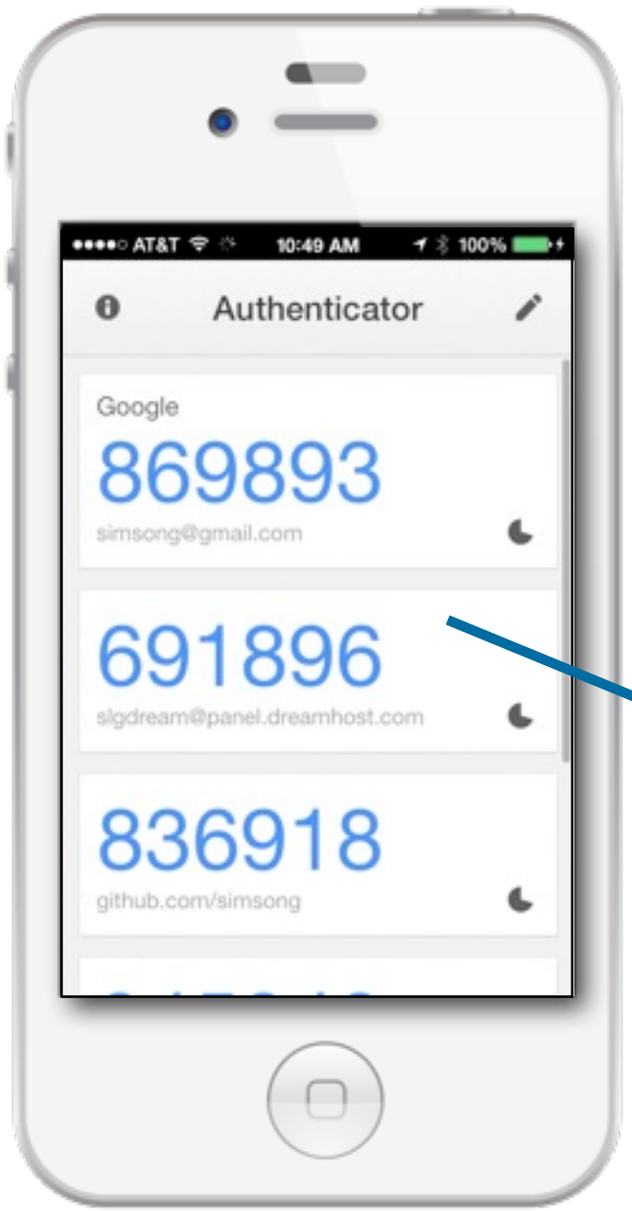


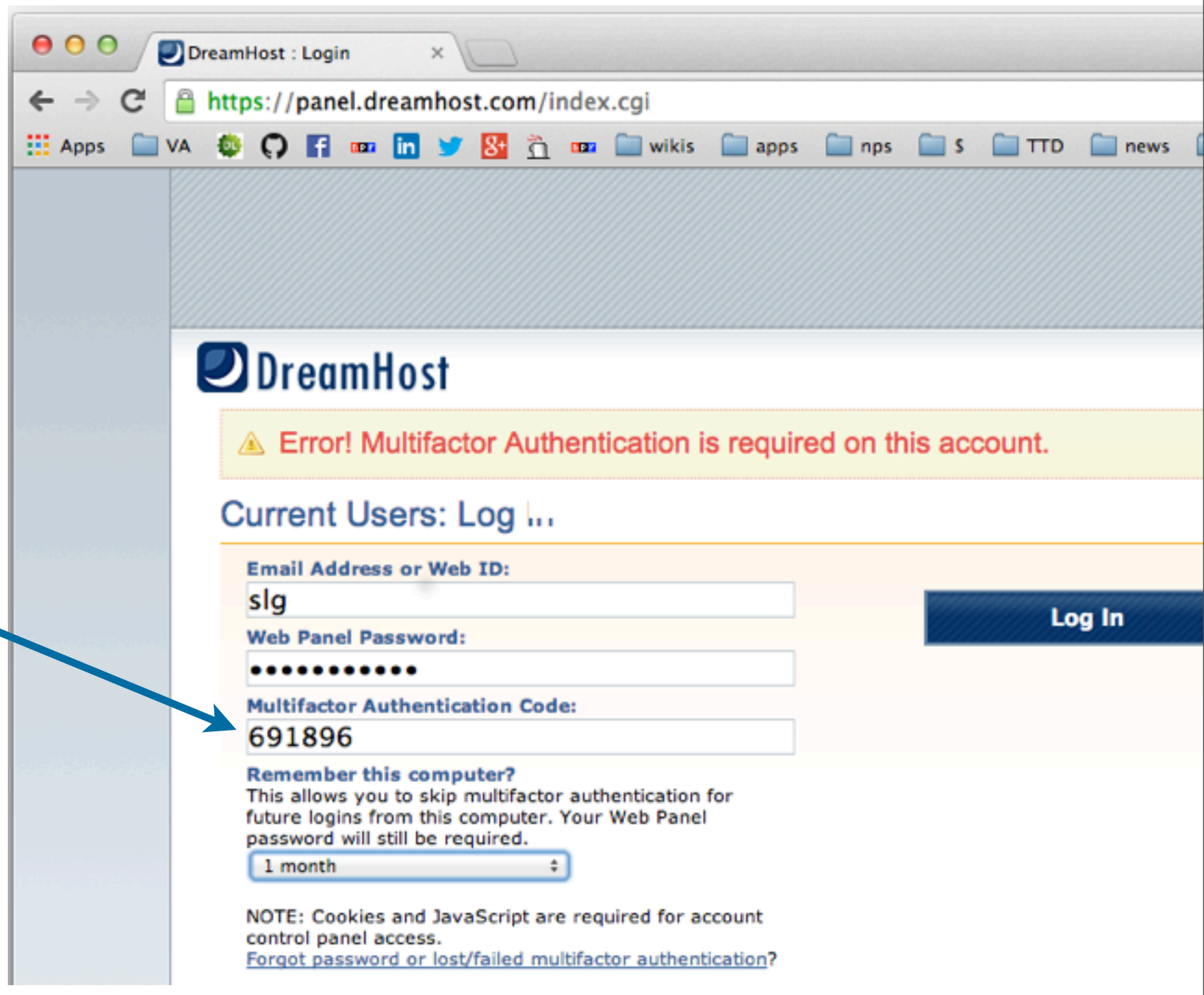
Most "SSL" websites only use it for logging in.

DNSSEC

Smart Cards

Example: Google Authenticator's 2-factor authentication protections against password stealing.





Example:
Apply “Recovery Oriented Computing” to security.

Recovery Oriented Computing [Stanford & Berkeley]:

- Systems that are isolated and redundant
- System-wide undo support
- Integrated Diagnostic support
- Online verification and recovery mechanisms
- Modularity, measurability and restorability

Applying to security:

- Pervasive use of digital signatures.
- Disconnected, offline storage.

We must address the non-technical factors that impact cyber security.

These factors reflect deep divisions within our society.

- ***Shortened*** development cycles
- ***Education:*** Not enough CS graduates; not enough security in CS.
- ***Labor:***
  - —***Immigration Policy:*** *Foreign students; H1B Visa*
  - —***HR:*** *Inability to attract and retain the best workers*
- ***Manufacturing Policy:*** Where we are building our computers.

Solving the cyber security mess requires addressing these issues.

Short development cycles

Insufficient planning:

- Security not “baked in” to most products.
- Few or no security reviews
- Little Usable Security

Insufficient testing:

- Testing does not uncover security flaws
- No time to retest after fixing

Poor deployment:

- Little monitoring for security problems
- Difficult to fix current system when new system is under development

Education is not supplying enough security engineers. Software engineers don't learn enough about security.

Security HR Pipeline

- High School → College → Graduate School → Career

It takes *years* to master security...

- Many professional programmers learn their craft in college.
- College English graduates: 16 years' instruction in writing
- College CS graduates: 4 years' instruction in programming

  —*Is it any wonder their code has security vulnerabilities?*
- 64% of the 2,500 vulnerabilities in the National Vulnerability Database in 2004 were caused by programming errors.

Forbes

Kashmir Hill, Forbes Staff

Welcome to The Not-So Private

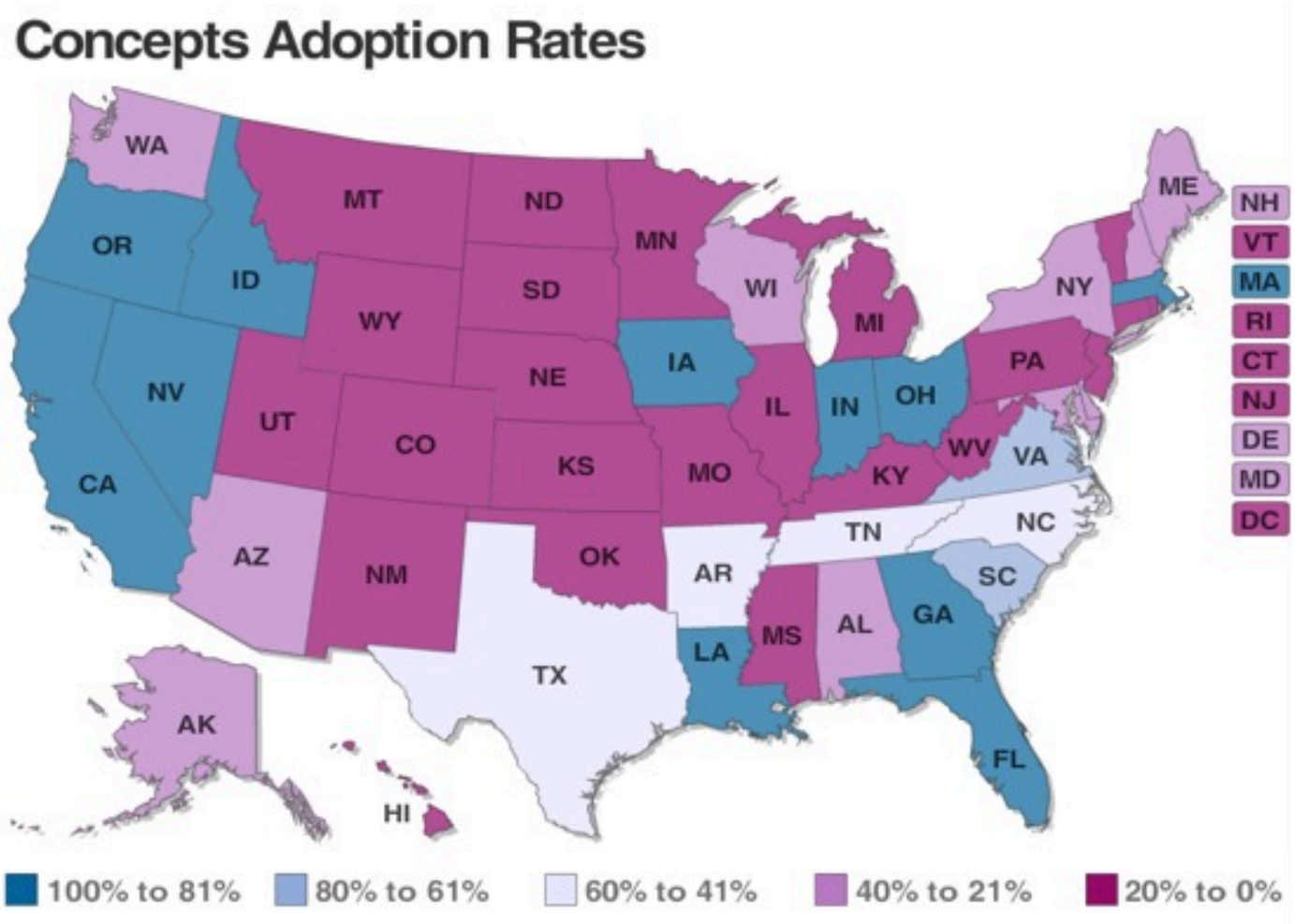
Follow (1,349) Follow

TECH | 5/09/2013 @ 4:51PM | 261,967 views

Snapchats Don't Disappear: Forensics Firm Has Pulled Dozens of Supposedly-Deleted Photos From Android Phones

http://www.forbes.com/sites/kashmirhill/2013/05/09/snapchats-dont-disappear/

73% of states require computer “skills” for graduation. Only 37% require CS “concepts”



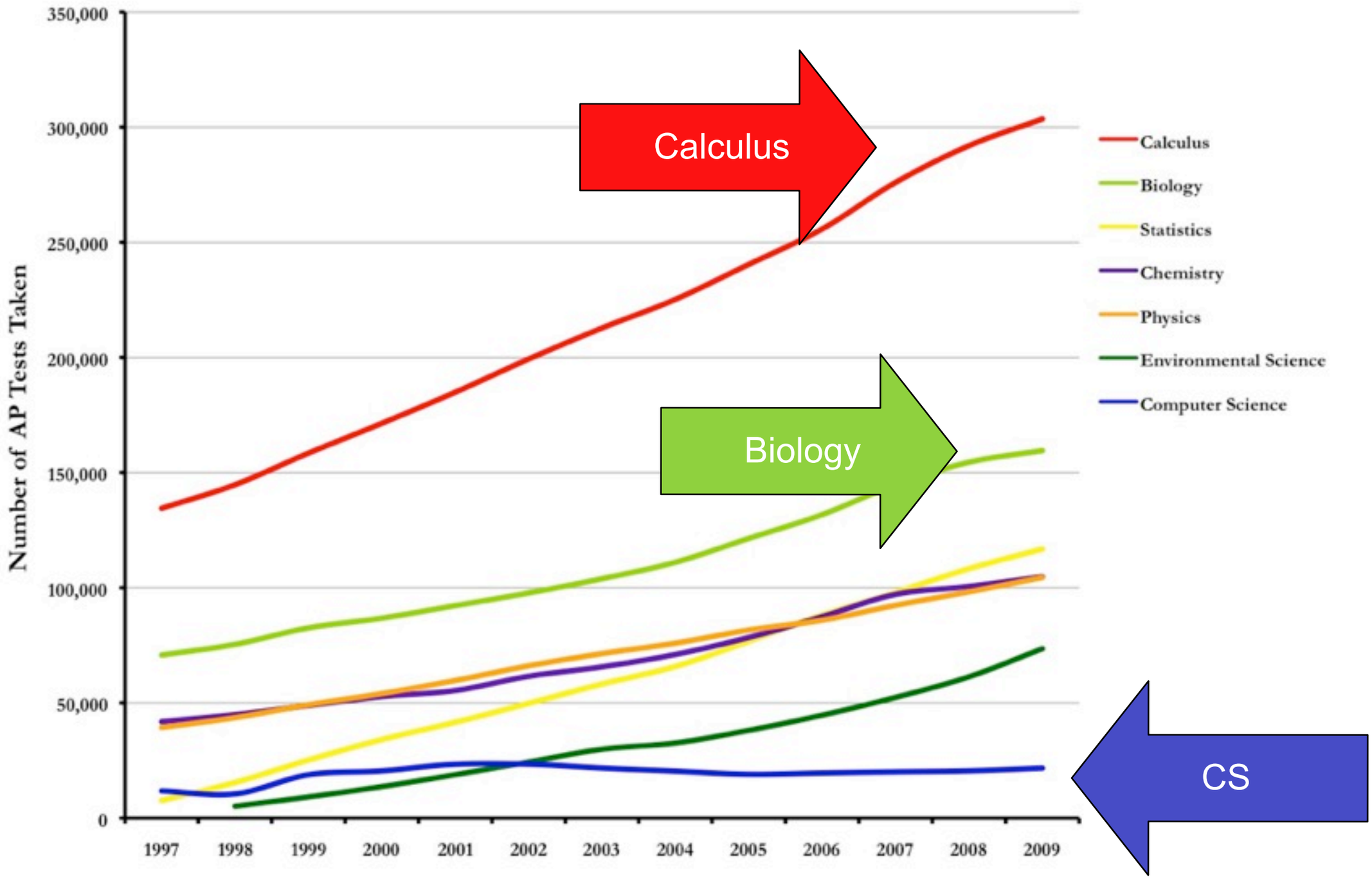
CS teachers are paid far less than CS engineers.

—*Salaries for beginning & average teachers lag CS engineers by 30%*

—*Adjusting for cost-of-living and shorter work week.*

- Linda Darling-Hammond, Stanford University, 2004
  http://www.srnleads.org/data/pdfs/ldh_achievemen_gap_summit/inequality_TCR.pdf

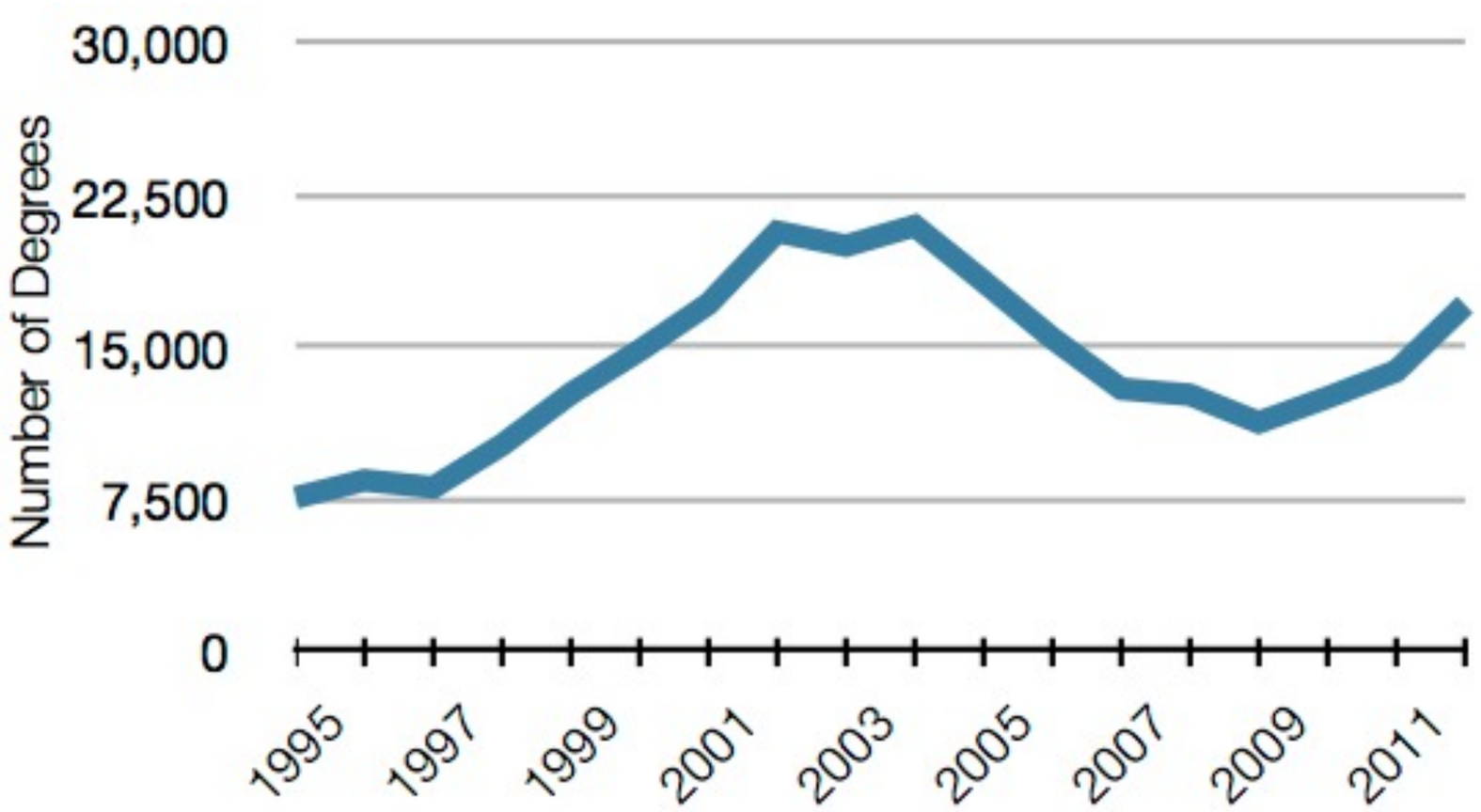
High school students are not taking AP computer science!



http://www.acm.org/public-policy/AP%20Test%20Graph%202009.jpg

Computer Science undergraduate enrollment has gone up for 4 years, but still not reached 2001-2004 levels

CRA is psyched at double-digit gains in recent years, but…



Source: Table 3: Bachelor's Degrees Awarded by Department Type

2013 CRA Taulbee Survey

http://cra.org/govaffairs/blog/2013/03/taulbeereport/

7% of Bachelor's degrees awarded to "nonresident alien" (12,596 to US citizens)

Table B3. Bachelor's Degrees Awarded by Ethnicity

	CS		CE		I		Total	
Nonresident Alien	619	6.8%	216	10.5%	98	4.1%	933	6.9%
Amer Indian or Alaska Native	39	0.4%	6	0.3%	12	0.5%	57	0.4%
Asian	1,477	16.3%	447	21.7%	341	14.2%	2,265	16.7%
Black or African-American	407	4.5%	107	5.2%	203	8.4%	717	5.3%
Native Hawaiian/Pac Islander	18	0.2%	4	0.2%	3	0.1%	25	0.2%
White	5,793	64.0%	1,154	55.9%	1,522	63.2%	8,469	62.6%
Multiracial, not Hispanic	130	1.4%	27	1.3%	26	1.1%	183	1.4%
Hispanic, any race	575	6.3%	102	4.9%	203	8.4%	880	6.5%
Total Residency & Ethnicity Known	9,058		2,063		2,408		13,529	
Resident, ethnicity unknown	732		117		89		938	
Residency unknown	1,259		176		73		1,508	
Grand Total	11,049		2,356		2,570		15,975	

—Most do not go on to advanced degrees.

54% of Master's degrees awarded to nonresident alien (4960 to US citizens)

Table M3. Master's Degrees Awarded by Ethnicity

	CS		CE		I		Total	
Nonresident Alien	4,123	62.3%	544	69.3%	397	19.8%	5,064	53.8%
Amer Indian or Alaska Native	10	0.2%	1	0.1%	9	0.4%	20	0.2%
Asian	484	7.3%	52	6.6%	213	10.6%	749	8.0%
Black or African-American	123	1.9%	8	1.0%	122	6.1%	253	2.7%
Native Hawaiian/Pac Island	9	0.1%	0	0.0%	0	0.0%	9	0.1%
White	1,725	26.1%	161	20.5%	1,144	57.0%	3,030	32.2%
Multiracial, not Hispanic	22	0.3%	1	0.1%	25	1.2%	48	0.5%
Hispanic, any race	123	1.9%	18	2.3%	96	4.8%	237	2.5%
Total Residency & Ethnicity Known	6,619		785		2,006		9,410	
Resident, ethnicity unknown	285		78		144		507	
Residency unknown	558		15		28		601	
Grand Total	7,462		878		2,178		10,518	

—We should let them stay in the country after they graduate

50% of PhDs awarded in 2012 to nonresident aliens

Table D3. PhDs Awarded by Ethnicity

	CS		CE		I		Total	
Nonresident Alien	763	51.3%	99	55.3%	32	26.9%	894	50.1%
Amer Indian or Alaska Native	1	0.1%	0	0.0%	1	0.8%	2	0.1%
Asian	168	11.3%	32	17.9%	27	22.7%	227	12.7%
Black or African-American	27	1.8%	1	0.6%	7	5.9%	35	2.0%
Native Hawaiian/Pac Islander	5	0.3%	0	0.0%	0	0.0%	5	0.3%
White	496	33.4%	45	25.1%	51	42.9%	592	33.2%
Multiracial, not Hispanic	5	0.3%	0	0.0%	0	0.0%	5	0.3%
Hispanic, any race	22	1.5%	2	1.1%	1	0.8%	25	1.4%
Total Residency & Ethnicity Known	1,487		179		119		1,785	
Resident, ethnicity unknown	25		1		5		31	
Residency unknown	94		14		5		113	
Grand Total	1,606		194		129		1,929	

—We did not train Russia's weapons scientists at MIT during the Cold War.

Just 67 / 1275 (5%) PhDs went into Information Assurance
15 professors & postdocs; 48 to industry & government

Table 14. Employment of New PhD Recipients By Specialty

	Artificial Intelligence	Computer-Supported Cooperative Work	Databases / Information Retrieval	Graphics/Visualization	Hardware/Architecture	Human-Computer Interaction	High-Performance Computing	Informatics: Biomedica/ Other Science	Information Assurance/Security	Information Science	Information Systems	Networks	Operating Systems	Programming Languages/ Compilers	Robotics/Vision	Scientific/ Numerical Computing	Social Computing/ Social Informatics	Software Engineering	Theory and Algorithms	Other	Total	
North American PhD Granting Depts.																						
Tenure-track	14	1	5	6	2	10	1	2	5	9	2	6	2	3	3	1	4	7	6	13	102	7.1%
Researcher	6	1	4	6	1	1	0	6	2	0	2	7	2	2	2	3	1	3	7	17	73	5.1%
Postdoc	38	1	12	17	4	12	0	20	7	5	2	12	7	7	14	6	3	10	30	34	241	16.8%
Teaching Faculty	2	1	1	0	0	1	0	1	1	2	1	1	1	1	0	0	3	4	4	4	28	2.0%
North American, Other Academic																						
Other CS/CE/I Dept.	3	0	4	1	1	1	4	2	2	0	5	6	1	0	0	0	0	3	1	18	52	3.6%
Non-CS/CE/I Dept.																						
North American, Non-Academic																						
Industry	64	2	49	46	41	24	20	17	40	5	6	67	29	22	25	6	12	86	32	83	676	47.2%
Government	7	0	5	2	6	2	5	3	8	1	2	1	0	0	2	4	1	4	2	5	60	4.2%
Self-Employed	0	0	0	1	0	1	0	1	0	0	2	2	2	0	1	0	0	1	1	1	13	0.9%
Unemployed	2	0	2	1	2	2	1	0	2	0	1	3	0	0	1	0	2	0	1	3	23	1.6%
Other	2	0	1	0	0	0	1	1	0	0	0	1	0	0	0	0	0	0	1	0	7	0.5%
Total Inside North America																						
	138	6	83	80	57	54	32	53	67	22	23	106	44	35	48	20	26	118	85	178	1,275	89.0%

Security should be taught to everyone, but we need specialists

Georgetown Prof: 50% of graduate students in sciences are foreigners because salaries aren't high enough.

"...the problem may not be that there are too few STEM qualified college graduates, but rather that STEM firms are unable to attract them.

Highly qualified students may be choosing a non-STEM job because it pays better, offers a more stable professional career, and/or perceived as less exposed to competition from low-wage economies."

RUTGERS
Edward J. Bloustein School of Planning and Public Policy
John J. Heldrich Center for Workforce Development

ISIM
Institute for the Study of International Migration
Edmund A. Walsh School of Foreign Service
at
Georgetown University

Steady as She Goes?
Three Generations of Students through the Science and Engineering Pipeline *

October 2009

B. Lindsay Lowell[a]
Hal Salzman[b,c]
Hamutal Bernstein[a]
with
Everett Henderson[c]

Paper presented at:
Annual Meetings of the
Association for Public Policy
Analysis and Management
Washington, D.C.

November 7, 2009

[a] Institute for the Study of International Migration, Georgetown University
B. Lindsay Lowell: lowellbl@georgetown.edu

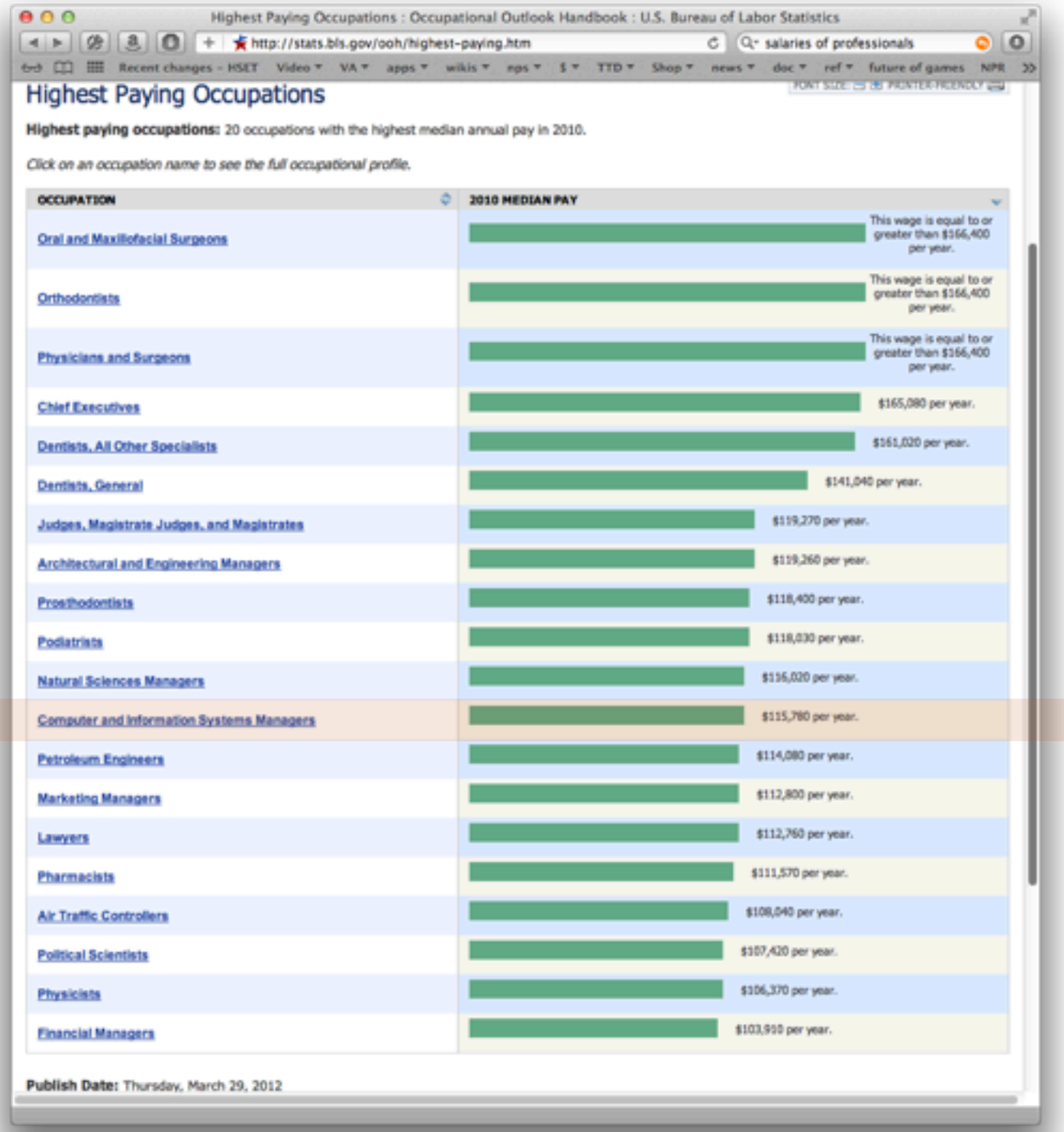
[b] Heldrich Center for Workforce Development
Bloustein School of Public Policy
Rutgers University &
[c] The Urban Institute
Hal Salzman: HSalzman@Rutgers.edu

* Michael Teitelbaum provided insightful comments on an earlier draft of this paper and on the research throughout the project. We appreciatively acknowledge the contributions to this paper by Katie Vinopal of the Urban Institute. Research for this paper was funded by the Alfred P. Sloan Foundation.

Bureau of Labor Statistics puts CS as 12th highest paying profession, after...

Highest paying occupations:

- Oral Surgeons > $166,400
- Orthodontists > $166,400
- Physicians and Surgeons >$166,400
- CEOs: $165,080
- Dentists: $161,020
- Judges: $119,260
- Architectural & Eng. Mgrs. $119,260
- Prosthodontists $118,400
- Podiatrists $118,030
- Natural Sci. Mgrs. $116,020
- Computer Scientists: $115,070
- Petroleum Engineers $114,080
- Marketing Managers $112,800
- Lawyers: $112,760



Manufacturing policy — The US did not buy WW2 aircraft from Germany

Boeing Whichata B-29 Assembly Line, 1944
http://en.wikipedia.org/wiki/File:Boeing-Whichata_B-29_Assembly_Line_-_1944.jpg

But we buy *nearly all* of our computers from China.

It's *easy* to put backdoors in hardware and software.

There is no obvious way to secure cyberspace.

We *trust* computers…

—*but we cannot make them trustworthy.*
(A "trusted" system is a computer that can violate your security policy.)

We know a lot about building secure computers...

—*but we do not use this information when building and deploying them.*

We know about usable security…

—*but we can't make any progress on usernames and passwords*

We should design with the assumption that computers will fail…

—*but it is cheaper to design without redundancy or resiliency.*

Despite the new found attention to cyber security,
our systems seem to be growing more vulnerable every year.

Backup Slides:

HCI-SEC

Major Themes in HCI-SEC Academic Research

UserAuthentication
- Text Passwords
- Graphical Authentication
- Biometrics
- Token-based Authentication
- CAPTCHAs

Email Security and PKI
- Automatic,Transparent Encryption

Anti-PhishingTechnology

Password Managers

Device Pairing

Web Privacy

Policy Specification and Interaction

Security Experts

Mobile Security and Privacy
- Location Privacy
- Application platforms
- Mobile authentication

Social Media Privacy

HCI-SEC Lessons and Challenges

Lessons Learned:

- Users need better information, not more information
- To make good decisions, users require clear context
- Plain Language Works,Even if it is less precise
- Where Possible, Reduce Decisions and Configuration Options
- Education Works, but cannot overcome economics

Research Challenges

- Authentication Challenges
- Administration Challenges
- Privacy Challenges
- Challenge of Modelling the Adversary
- The Challenge of Social Media and Social Computing
- Teaching Challenges

HCI-SEC Conclusion: The Next 10 years

More HCI-SEC Research Centers

More HCI-SEC ResearchTargets

Increased Researching on Nudges and Pusuasion

Increased Emphasis on Offensive Work

Increased demand for HCI-SEC from non-technical sectors

Backup Slides:

Insider Threat

DETECTING THREATENING INSIDERS WITH LIGHTWEIGHT MEDIA FORENSICS

Naval Postgraduate School &
The University of Texas at San Antonio

Dr. Simson Garfinkel (NPS) & Dr. Nicole Beebe (UTSA)

8am, Wednesday November 13th, 2013

Team Profile

Naval Postgraduate School

- Simson L. Garfinkel
  Assoc. Prof
  Computer Science
  —*simsong@acm.org*
  —*+1.202.649.0029*

The University of Texas at San Antonio

- N. Beebe, Asst. Prof.
  Info Systems/Cyber Security
  —*Nicole.Beebe@utsa.edu*
  —*+1.210.269.5647*

The current approaches for finding hostile insiders are based on "signatures."

Sample signature to find a problem employee:

(CERT 2011)

- ***if the mail is from a departing insider***
- ***and the message was sent in last 30 days***
- ***and the recipient is not in organization's domain***
- ***and the total bytes summed by day is more than X,***

➜ ***send an alert to security operator***

These signatures are typically hand written.

—*Brittle*

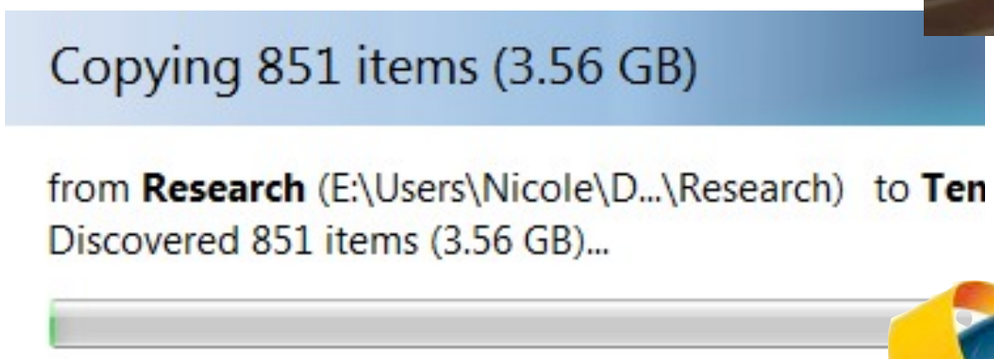
—*Don't scale*

—*Miss new patterns*

We propose a new approach for finding threatening insiders—storage profile anomalies.

Hypothesis 1:
Some insiders hoard before exfiltration

- Manning
- Snowden



We also want to detect other kinds of illegal employee activity.

Hypothesis 2:
Some illegal activity has storage indicators:

- Contraband software (hacking tools) and data
- Large amount of:
  - —*graphics*
  - —*PII; PHI; account numbers*
  - —*Encrypted data*
- Stolen documents

Illegal employee activity is:

- Bad for business
- Exploitation threat
- Fraud risk

CNN Justice

Pentagon reopening probe into employees allegedly tied to child porn

By Adam Levine, CNN
September 16, 2010 11:59 a.m. EDT

The Defense Department will review 264 cases of possible trafficking in child pornography.

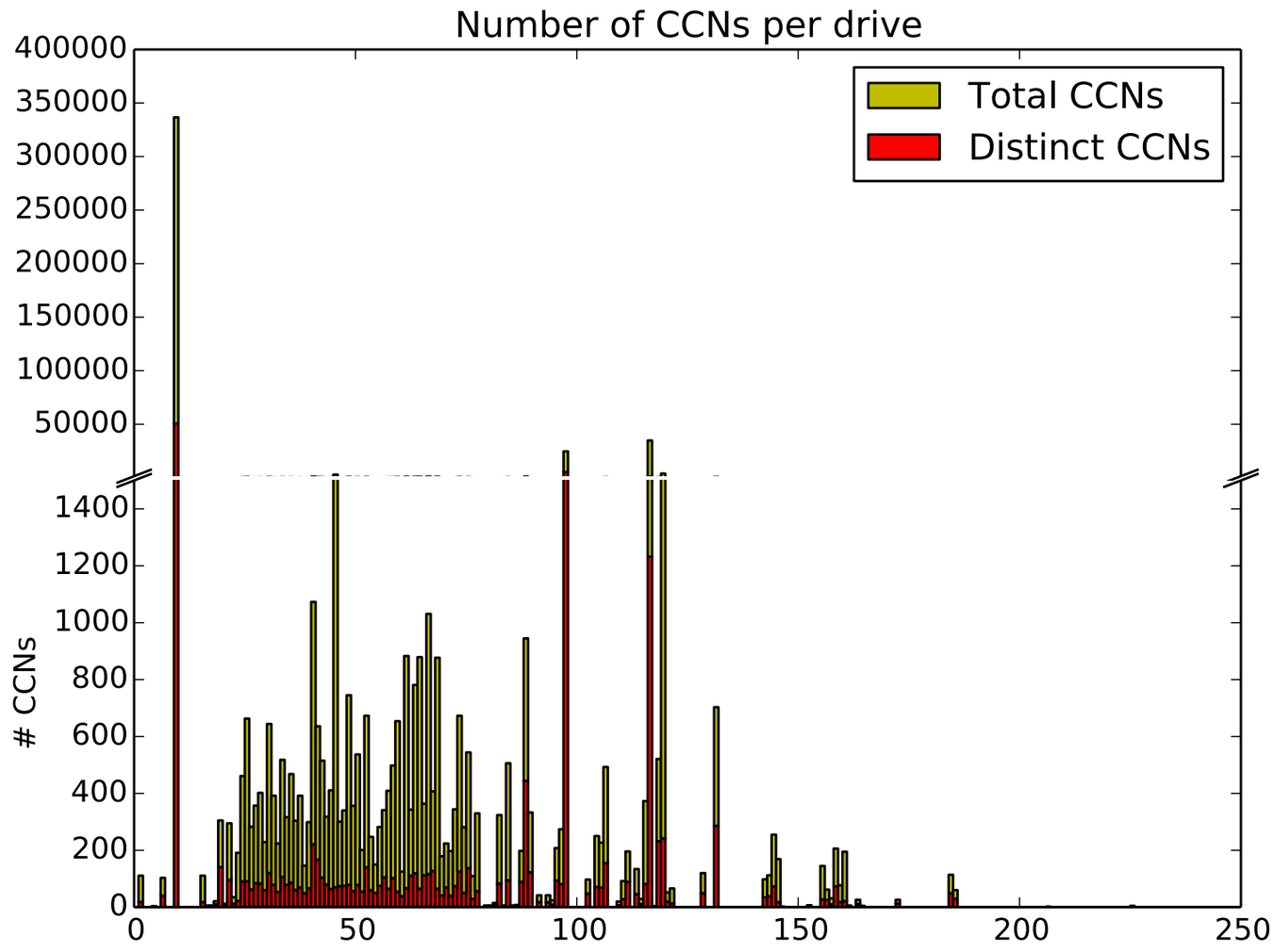
(CNN) -- The Defense Department will reopen its investigation into employees who are alleged to have downloaded child pornography, a spokesman said Wednesday.

The Pentagon's Defense Criminal Investigative Service will review 264 cases, according to spokesman Gary Comerford. The department had stopped the reviews because of a lack of resources, he said.

Our plan: look for storage devices that are different than their peers.

We build a “storage profile” from features:

- # of credit card numbers, phone #s; SSNs, DOBs, etc.
- % pictures; %video
- % Doc files; %PDFs;



“Different” relative to:

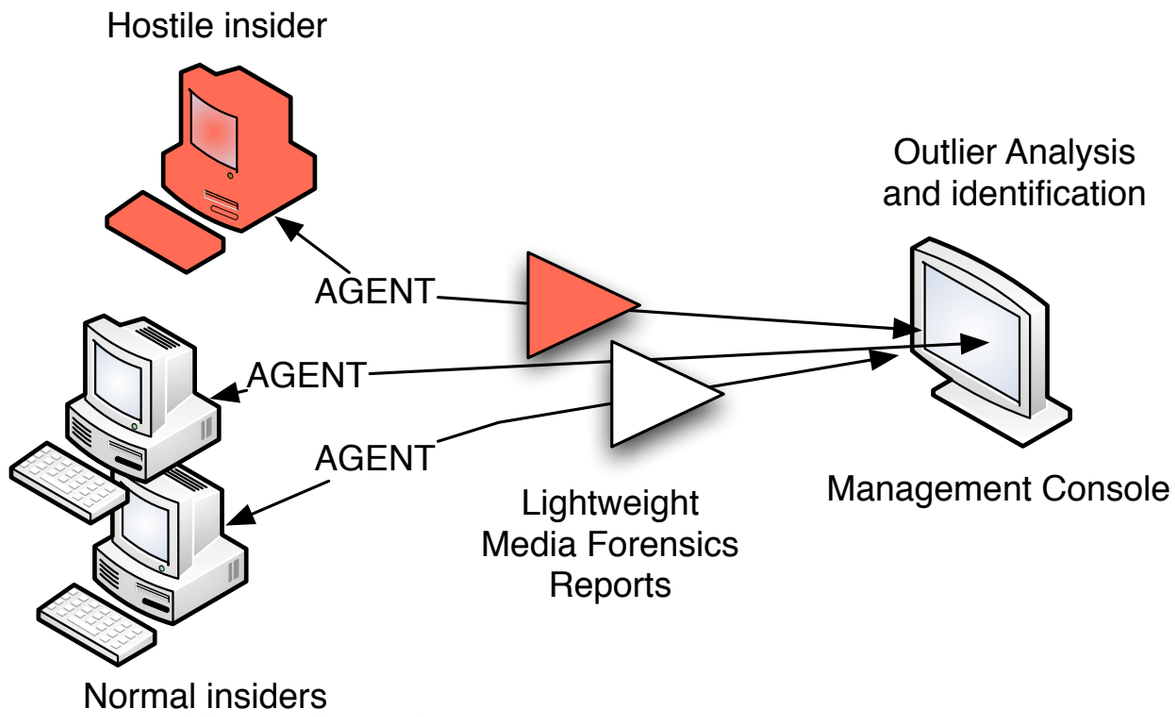
- User’s history
- User’s organization
- Others in role.

Garfinkel, S. and Shelat, A., "Remembrance of Data Passed: A Study of Disk Sanitization Practices," IEEE Security & Privacy, January/February 2003.

Our approach:
Collect “storage profiles” and look for outliers.

We profile storage on the hard drive/storage device:

- Allocated & “deleted” files; Unallocated space (file fragments)



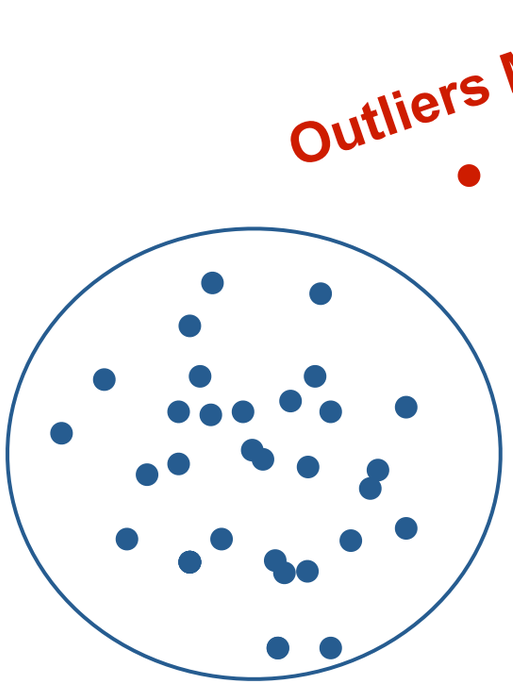
Statistical profile is collected:

- Frequently, at “random” times
- Securely — by going to raw media
- Centrally — at management console

We cluster the storage profiles to find “outliers.”

What’s an outlier?

- Something that’s different from its peers
- Something different from its own history



“Normal” Storage Profile

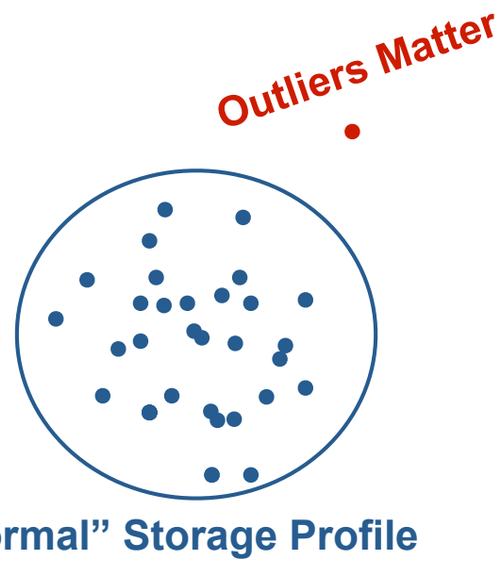
Outlier detection should have significant benefits:

- Not signature based
- Not reliant on access patterns
- Not reliant on policy definition, discovery, auditing

Design constraints:

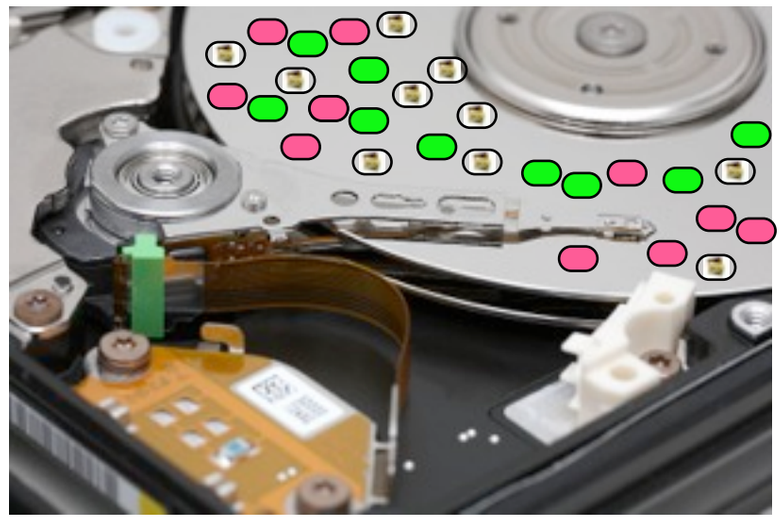
- Agent must be scalable and cannot interfer with operations
  - —*Desktop: background process, samples disk data*
  - —*Network load: small, aggregated data transfer*
  - —*Management console: scalable algorithms used*

- Must work with isolated systems
- Must be OS agnostic
- Must includes deleted data in collection/analysis



Our system has three parts:

1. Sample disk to collect desired data
   - bulk_extractor
     — *a lightweight media forensics tool*

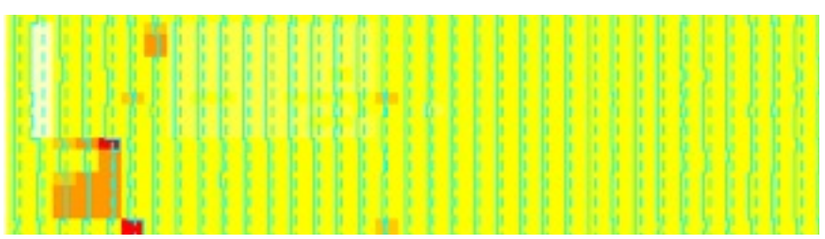


Garfinkel, Simson, Digital media triage with bulk data analysis and bulk_extractor. Computers and Security 32: 56-72 (2013)

2. Client-server, enterprise response framework
   - Google Rapid Response (GRR)

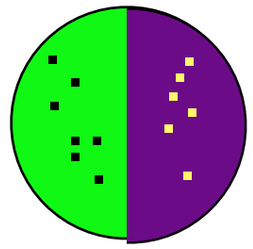
grr
GRR Rapid Response is an Incident Response Framework

3. Anomaly detection agent
   - Univariate and multivariate outlier detection



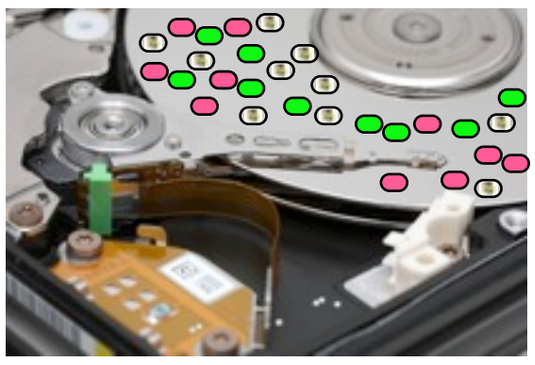
Random sampling is a great way to analyze data.

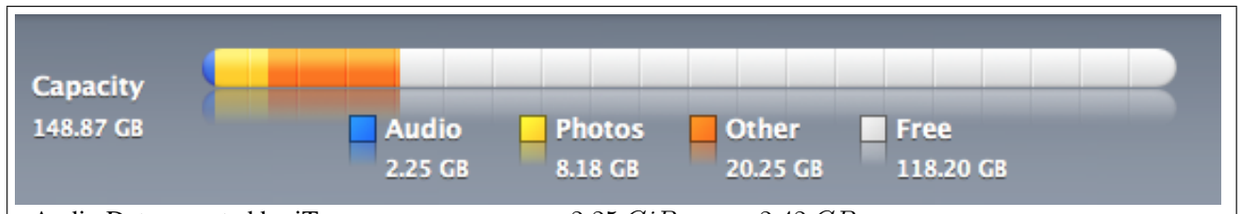
Simple random sampling can determine % free space



Garfinkel, Simson, Vassil Roussev, Alex Nelson and Douglas White, Using purpose-built functions and block hashes to enable small block and sub-file forensics, DFRWS 2010, Portland, OR

Data characterization can determine the *kind* of stored data

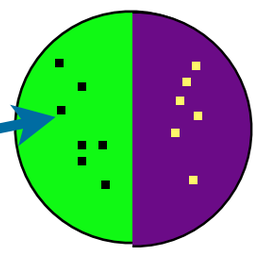




Audio Data reported by iTunes:	2.25 GiB	2.42 GB	
MP3 files reported by file system:		2.39 GB	
Estimated MP3 usage with random sampling :		2.49 GB	10,000 random samples
		2.71 GB	5,000 random samples

Sector hashing can identify *specific target files*

Young J., Foster, K., Garfinkel, S., and Fairbanks, K., Distinct sector hashes for target file detection, IEEE Computer, December 2012



It takes 3.5 hours to read a 1TB hard drive.

In 5 minutes you can read:

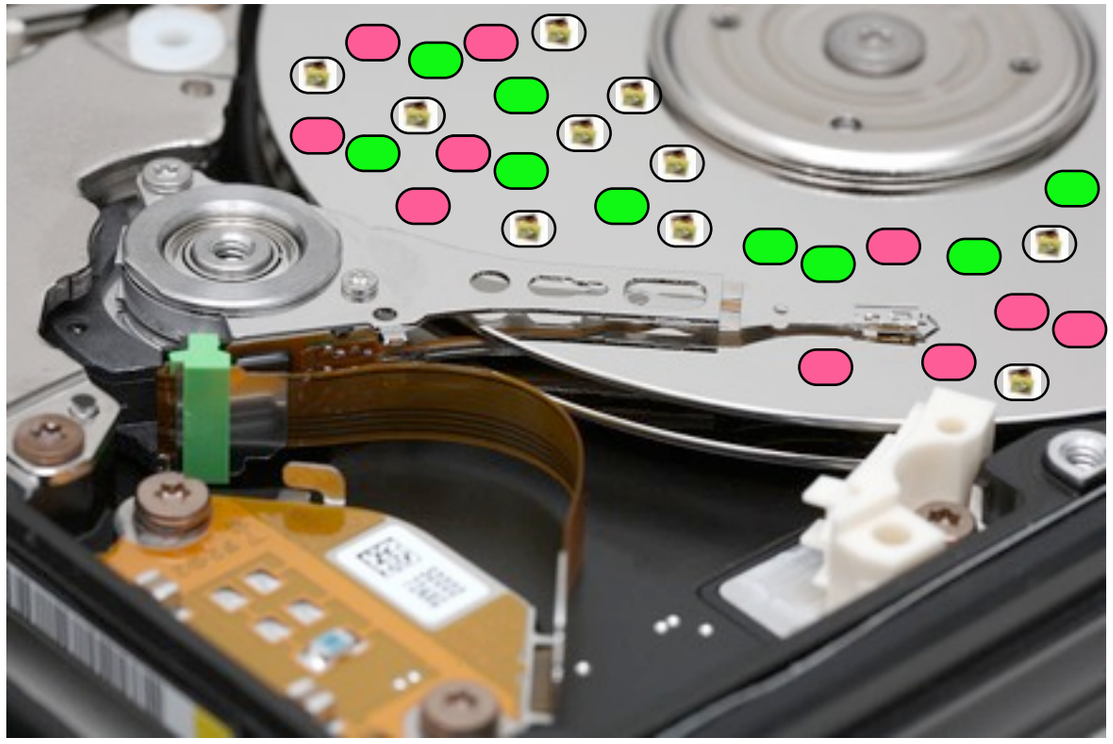
- 36 GB in one strip
- 100,000 randomly chosen 64KiB strips (assuming 3 msec/seek)

			
Minutes	208	5	5
Data	1 TB	36 GB	6.5 GB
# Seeks	1	1	100,000
% of data	100%	3.6%	0.65%

The statistics of a *randomly chosen sample* predict the *statistics of a population.*

US elections can be predicted by sampling thousands of households:

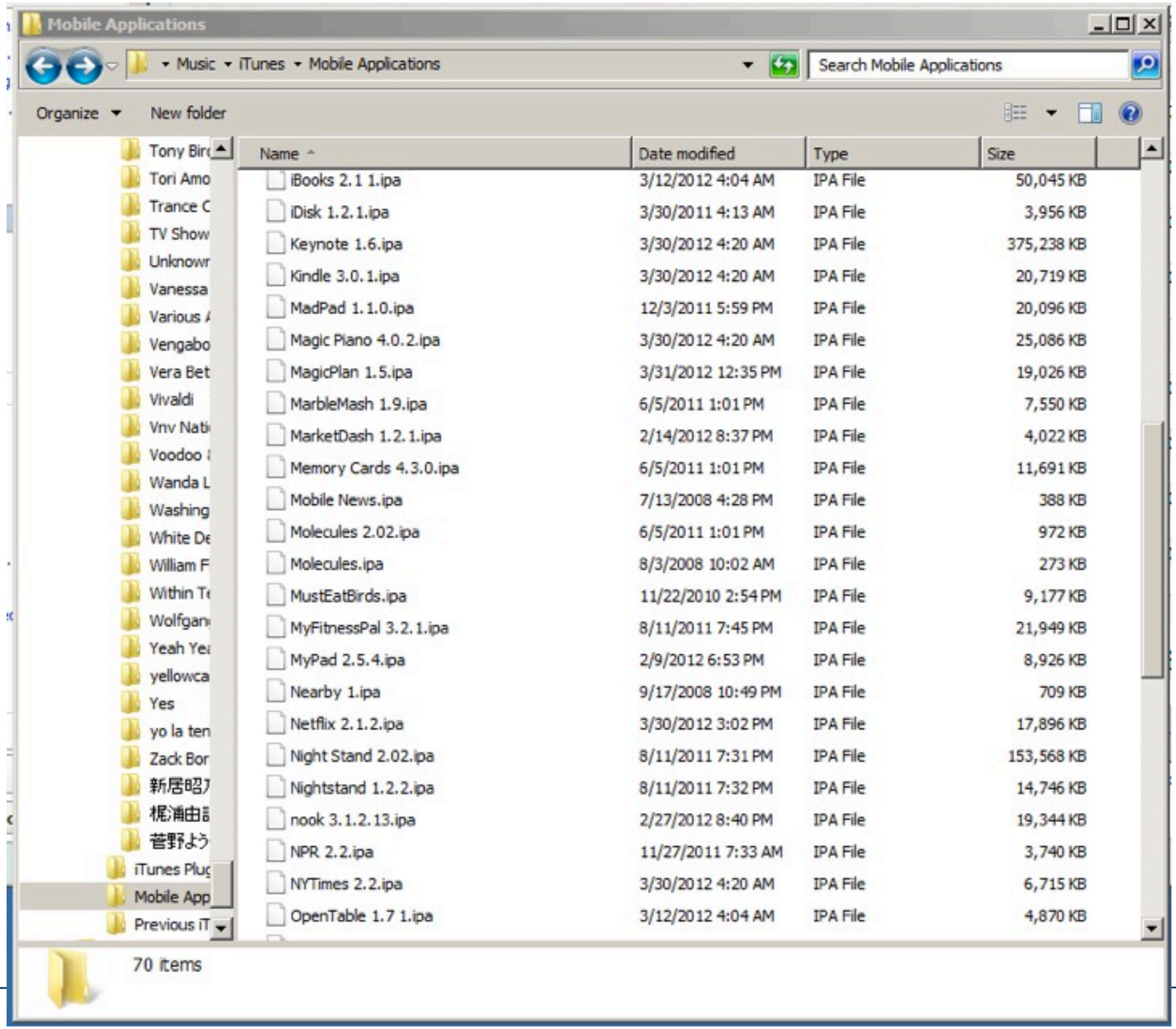
Hard drive contents can be predicted by sampling thousands of sectors:



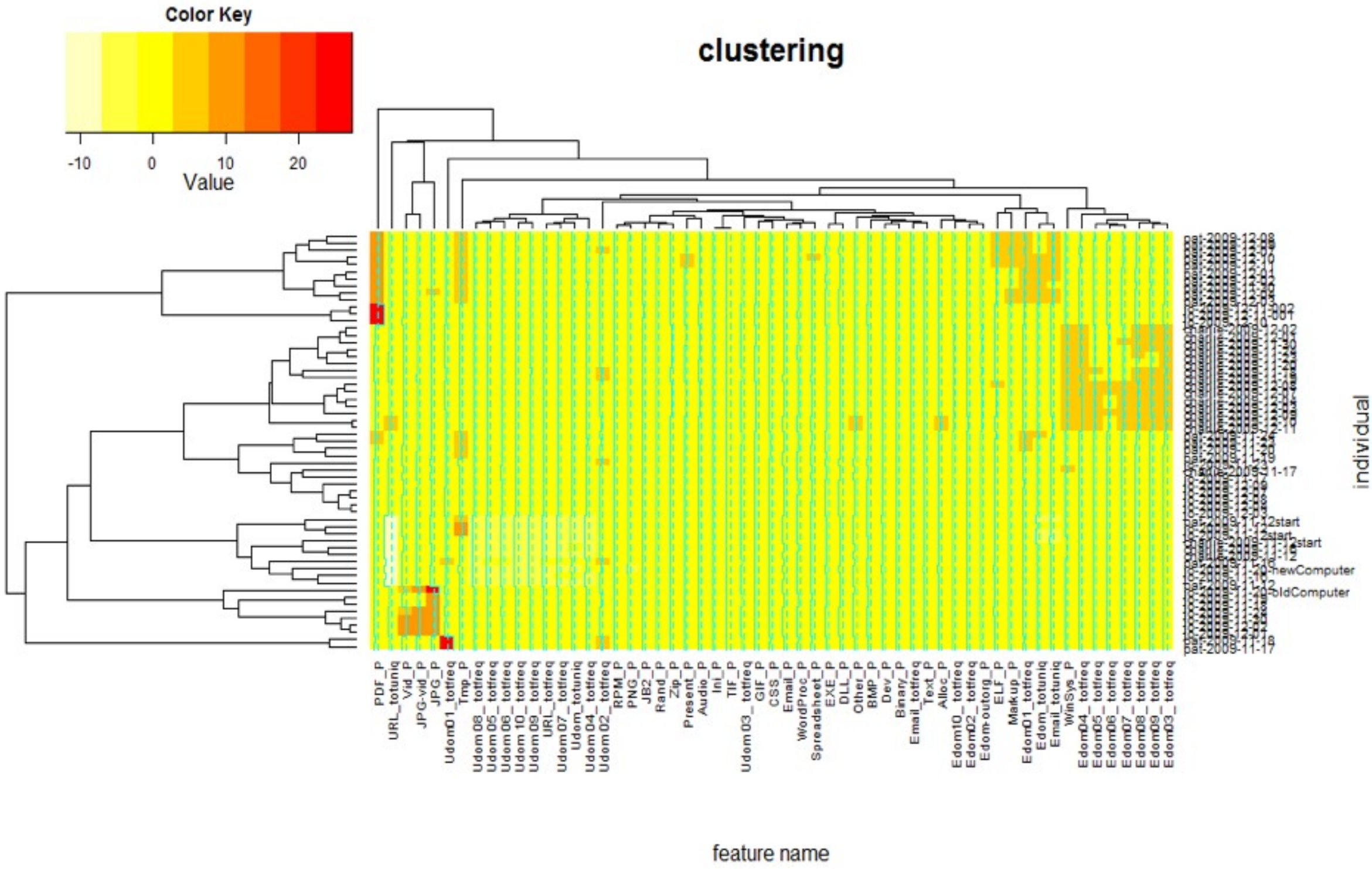
The challenge is identifying *likely voters.*

The challenge is *identifying the sector* content that is sampled.

We think of computers as devices with *files*.



This heatmap of anomalies let an analyst easily identify clusters and outliers.



Current status —

bulk_extractor updated v1.4 just released

- Added features & GRR integration preparation

Sceadan data type classifier updated v1.2 released

Extraction, transformation, loading of datesets

- M57 Patents (digitalcorpora.org) case

Progress on anomaly detection algorithm

- Real Data Corpus extraction, translation and loading near complete
- Theoretical development
- Empirical data descriptive analyses (test assumptions)
- Univariate anomaly detection performing well on synthetic data set

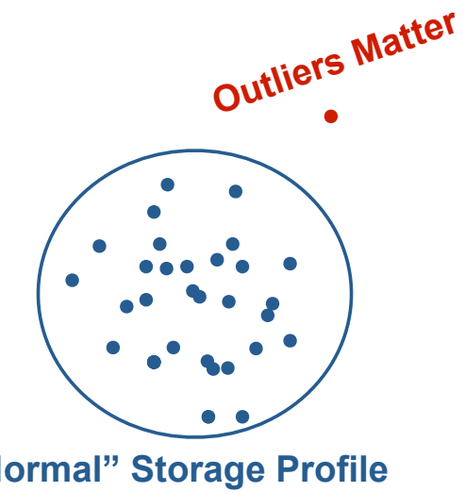
We are in year 1 of a 3-year effort.

	NPS Lead	UTSA Lead
Year 1	bulk_extractor upgrades	Outlier detection algorithm Synthetic data experimentation Real Data Corpus experimentation
Year 2	Integrate GRR Develop/test management console	Develop/test data outlier detection Develop/test visualization component
Year 3	Large-scale testing on partner net	Final dev. of outlier detection algorithm Final dev. of visualization agent

Many challenges remain.

"Anomalous" suggests "normal" exists

- Large, diverse, dislocated organizations
- High fluidity and variety in workforce
- Remote, mobile, multi-device access requirements
- Uninterruptible, critical computational operations



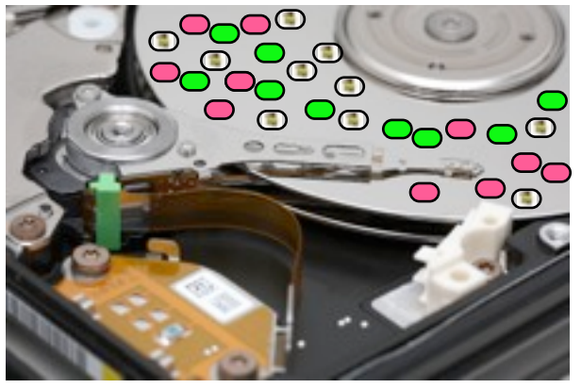
Clustering algorithm selection/development

- Accuracy and speed trade-off of extant algorithms
- Develop combinatorial algorithm to improve accuracy
- Need for automated parameter selection amidst noise
- Feature selection

Engineering of visualization component

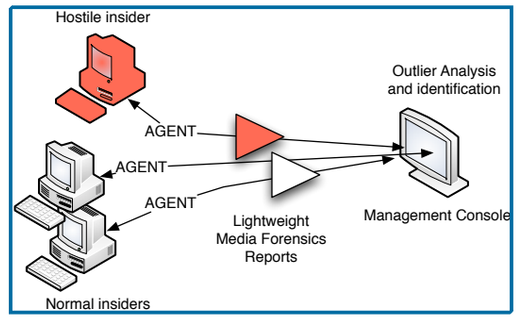
In conclusion, we are developing a system that uses "lightweight media forensics" to find hostile insiders.

We use random sampling to build a storage profile of media



We collect these profiles on a central server

We cluster & data mine to find outliers.



Contact:

- Simson L. Garfinkel simsong@acm.org
- Nicole Beebe *Nicole.Beebe@utsa.edu*